ESTUDIO ALGEBRAICO DE LOS NÚMEROS DUALES

HAYDEE JIMÉNEZ TAFUR

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ D.C.
2006

ESTUDIO ALGEBRAICO DE LOS NÚMEROS DUALES

HAYDEE JIMÉNEZ TAFUR

Trabajo de grado para optar al título
de Licenciado en Matemáticas.

Asesor
CARLOS JULIO LUQUE ARIAS
Profesor Departamento de Matemáticas

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ D.C.
2006

A mi gran Amigo T.

AGRADECIMIENTOS

Agradezco al profesor Carlos Julio Luque Arias, por haber dirigido mi trabajo de grado y contribuido en mi formación profesional y personal.

A mi familia, por su constante apoyo.

RESUMEN ANALÍTICO

TIPO DE DOCUMENTO: Tesis de Grado.

ACCESO AL DOCUMENTO: Universidad Pedagógica Nacional.

TÍTULO: Estudio algebraico de los números duales.

AUTOR: JIMÉNEZ TAFUR, Haydee.

PUBLICACIÓN: Bogotá, Universidad Pedagógica Nacional, 2006, 99 páginas.

UNIDAD PATROCINANTE: Universidad Pedagógica Nacional, Facultad de Ciencia y Tecnología, Departamento de Matemáticas.

PALABRAS CLAVES: Números duales, elementos nilpotentes, anillo conmutativo con unidad, anillo de polinomios, subanillos, ideales, isomorfismos, anillo cociente.

DESCRIPCIÓN: Este documento muestra un estudio algebraico del anillo D de los números duales y del anillo de polinomios con coeficientes en los números duales. Tiene como propósito mostrar un ejemplo diferente a los usuales, donde buena parte de los teoremas del álgebra que son presentados en los libros de texto habituales, están dados para estructuras menos generales que la de anillo, por ejemplo los anillos de polinomios se tratan suponiendo que los coeficientes están en un campo.

FUENTES:

Bibliografía: Se consultaron 13 documentos entre libros y notas de clase referentes a la teoría de anillos y números duales, y un sitio en internet especializado en matemáticas.

CONTENIDOS

Objetivo General.

Elaborar un documento donde se recopile el estudio algebraico de los *Números Duales* teniendo en cuenta, estudios previos sobre Teoría de anillos.

Capítulo I. El anillo de los números duales

En el capítulo 1 se inicia con una presentación de la estructura de *-Álgebra de los números duales; se presentan enseguida diferentes representaciones que permiten la definición de potencias racionales de números duales, lo que exige una extensión de su estructura a un anillo de números duales con coeficientes complejos.

Seguidamente se estudian la función exponencial dual y la función logaritmo dual que permiten la definición de potencias duales de un número dual; luego se estudian ecuaciones en los números duales haciendo un estudio detallado de la ecuación de segundo grado.

Finalmente se define una relación de preorden para los números duales que es monótona para la adición y multiplicación y se estudian los subanillos e ideales de los números duales.

Capítulo II. El anillo de polinomios $D[Z]$

En el capítulo 2, se presenta el anillo de las series formales con coeficientes en D y con éste el anillo de los polinomios donde se estudian sus unidades, asociados y divisibilidad; mostrando que se cumple el algoritmo de la división y los teoremas del residuo y del factor; finalizando con la presentación de los ideales en $D[Z]$.

CONCLUSIONES:

El anillo de los números duales es un ejemplo interesante que permite ilustrar situaciones algebraicas que no son frecuentes en la teoría de anillos y campos que se estudia en la Licenciatura en Matemáticas de la Universidad Pedagógica Nacional, un ejemplo de ello es que a pesar de que D no es un dominio de integridad la propiedad cancelativa es válida para todos los elementos no nilpotentes; la función logaritmo, que en el caso de los números complejos tiene varias ramas, lo que dificulta su estudio y aplicación, en los números duales es una función biyectiva; en el anillo de polinomios con coeficientes en los números duales existen polinomios no constantes que tienen inverso multiplicativo, polinomios con infinitas raíces diferentes y el grado del producto de dos polinomios no en todos los casos es igual a la suma de los grados de los factores.

CONTENIDO

INTRODUCCIÓN

El presente trabajo hace un estudio algebraico del anillo *D* de los números duales y del anillo de polinomios con coeficientes en los números duales. Tiene como propósito mostrar un ejemplo diferente a los usuales, donde buena parte de los teoremas del álgebra que son presentados en los libros de texto habituales[1], están dados para estructuras menos generales que la de anillo, por ejemplo los anillos de polinomios se tratan suponiendo que los coeficientes están en un dominio de integridad o en un campo.

Otro propósito planteado es desarrollar actividad matemática en el sentido de ejercitar procesos de creación, discusión, proposición de algoritmos, manejo de teorías, formulación de conjeturas y en general, actividades características del trabajo matemático, que son fundamentales en la formación de un docente como matemático elemental; a este respecto se propusieron teoremas inéditos como: 1.21, 1.22, 1.23, 1.23, 1.25, 1.26, 1.27, 1.28, 1.29, 1.30, 1.31, 1.32, 1.33, 1.34, 1.35, 1.36, 1.37, 1.38, 1.39, 1.40, 1.41, 1.42, 1.43, 1.44, 1.45, 1.46, 1.47, 1.48, 1.49, 1.50, 1.51, 1.52, 1.53, 1.54, 1.57, 1.58, 1.59, 1.61, 1.62, 1.63, 1.64, 1.68, 1.69, 1.70, 1.71, 1.72, 1.75, 1.77, 2.3, 2.4, 2.5, 2.14, 2.15, 2.16, 2.20, 2.21, 2.24, 2.25, 2.26, 2.27, 2.28, 2.29, 2.30, 2.31, 2.32.

Se realizó un estudio sobre los polinomios irreducibles en $D[Z]$ obteniéndose una conjetura de la que no se consiguió una demostración completa cuyo bosquejo se presenta al final del capítulo 2.

[1] Por ejemplo en ALBIS, V. *Temas de aritmética y álgebra*. Bogotá, Universidad Nacional de Colombia. 1984. pp. 23 – 44., HERSTEIN, I. *Álgebra moderna*. México, F. Trillas. 1970. pp. 136 – 153., FRALEIGH, J. *A first course in abstract algebra. Sixth edition*. New York, Addison Wesley. 1999. pp. 285 – 308.

En el capítulo 1 se inicia con una presentación de la estructura de *-Álgebra de los números duales; se presentan enseguida diferentes representaciones que permiten la definición de potencias racionales de números duales, lo que exige una extensión de su estructura a un anillo de números duales con coeficientes complejos.

Seguidamente se estudian la función exponencial dual y la función logaritmo dual que permiten la definición de potencias duales de un número dual; luego se estudian ecuaciones en los números duales haciendo un estudio detallado de la ecuación de segundo grado.

Finalmente se define una relación de preorden para los números duales que es monótona para la adición y multiplicación y se estudian los subanillos e ideales de los números duales.

En el capítulo 2, se presenta el anillo de las series formales con coeficientes en D y con éste el anillo de los polinomios donde se estudian sus unidades, asociados y divisibilidad; mostrando que se cumple el algoritmo de la división y los teoremas del residuo y del factor; finalizando con la presentación de los ideales en $D[Z]$.

CAPÍTULO 1

EL ANILLO DE LOS NÚMEROS DUALES

1.1. OPERACIONES EN LOS NÚMEROS DUALES

Definición 1.1: Sea D el plano cartesiano R^2, con la adición de (a, b) y (c, d) definida componente a componente,

$$(a,b)(c,d) = (a + c,\ b + d)$$

y la multiplicación definida por

$$(a, b)(c, d) = (ac, ad + bc).$$

Definición 1.2: Dos elementos $z = (a, b)$ y $w = (c, d)$ en D son iguales si y sólo si $a = c$ y $b = d$.

Teorema[2] *1.1*: Con las dos operaciones anteriores D es un *anillo conmutativo*, con elemento idéntico (1, 0). A esta estructura se le conoce como *Números Duales* o *Números de Study*[3].

El conjunto de los números duales con la adición y la multiplicación *no forman un dominio de integridad*, debido a la existencia de elementos divisores de cero, es decir elementos

[2] Todos los teoremas que se enuncian sin demostración son consecuencia directa de las definiciones.
[3] YAGLOM, I. (1979) *A simple non Euclidean geometry and its physical basis*, Springer Verlag, New York, p. 265.

diferentes de (0, 0) tales que su producto es (0, 0). En D los divisores de cero corresponden a elementos de la forma (0, b) para cualquier número real b.

Teorema 1.2: La propiedad cancelativa se cumple en elementos de la forma $z = (a, b)$ con $a \neq 0$.

Demostración:
Si $z_1, z_2, z_3 \in D$ y $z_2 = (a, b)$, $z_1 = (x, y)$, $z_3 = (u, v)$ con $a \neq 0$:

$$z_1 z_2 = z_3 z_2$$

$$(z_1 - z_3) z_2 = (0, 0)$$

Donde $(z_1 - z_3) = w = (c, d)$, entonces

$$z_2 w = (ac, ad + bc) = (0, 0)$$

y por definición de igualdad entre números duales se tiene que:

$$ac = 0$$

$$ad + bc = 0$$

como $a \neq 0$ y a, b, c, d son números reales, se obtiene que $c = 0$ y $d = 0$.

Entonces

$$z_1 - z_3 = (x - u, y - v) = (0, 0)$$

luego $x = u$, $y = v$ y

$$z_1 = z_3.$$

Si $z_2 = (0, b)$, $z_1 = (x, y)$, $z_3 = (u, v)$, $b \neq 0$, se tiene que:

$$z_1 z_2 = z_3 z_2$$

$$(x, y)(0, b) = (u, v)(0, b)$$

$$(0, xb) = (0, ub)$$

Luego

$$xb = ub$$

$$x = u$$

Entonces si $z_1 z_2 = z_3 z_2$ y z_2 es nilpotente, sólo se puede asegurar que la primera componente de z_1 es igual a la de z_3.

Teorema 1.3: El anillo de los números duales es de característica 0.

Demostración:
Dado un entero positivo m tal que $m(1, 0) = (0, 0)$ implica que $m = 0$.

Teorema 1.4: El conjunto de los números duales de la forma $(a, 0)$ es isomorfo con los números reales.

Demostración:
La función

$$\theta : R \to D$$
$$a \mapsto (a,0)$$

es un homomorfismo inyectivo entre R y D, ya que

$$\theta(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \theta(a) + \theta(b)$$

$$\theta(ab) = (ab, 0) = (a, 0)\,(b, 0) = \theta(a)\;\theta(b)$$

y el núcleo de θ es igual al conjunto cuyo único elemento es 0. Así, R ≅ img(θ).

Teorema 1.5: *D* tiene estructura usual de *espacio vectorial real* de dimensión 2.

Si $n = (0, 1)$ y se nota $x(1, 0) = (x, 0)$ con el número real x, se escribe $(x, y) = x + yn$ con $n^2 = 0$.

Teorema 1.6: *D* es un *álgebra asociativa.*

Demostración:
D es un anillo conmutativo con unidad y la multiplicación por escalar y el producto son compatibles, es decir:

$$a(zw) = (az)w = z(aw) \quad a \text{ en R}; \quad z, w \text{ en } D.$$

Definición 1.3: El conjugado de un número dual $z = (a, b)$ es $\bar{z} = (a, -b)$.

Teorema 1.7: El álgebra asociativa *D* con la función definida por

$$\bar{}\,: D \to D$$

que a cada $z = (a, b)$ le asigna su conjugado dual $\bar{z} = (a, -b)$, es una $*$*–Algebra*[4].

Teorema 1.8: Para todo z en D, se cumple que $\overline{(\bar{z})} = z$.

[4] *D* no es una C*–Álgebra porque su seminorma no es una norma.

Teorema 1.9: Para todo z, w en D, se tiene que $\overline{(zw)} = \bar{z}\bar{w}$.

Demostración:
Dado $z = (a, b)$ y $w = (c, d)$ en D, el producto es

$$zw = (ac, ad + bc),$$

su conjugado es

$$\begin{aligned}\overline{zw} &= (ac, -(ad + bc)) \\ &= (ac, -ad - bc)\end{aligned}$$

y por definición de multiplicación en D y definición de conjugado

$$\begin{aligned}\overline{zw} &= (a, -b)(c, -d) \\ &= \bar{z}\bar{w}.\end{aligned}$$

Teorema 1.10: Para todo z, w en D y a en R, se tiene que $\overline{(az + w)} = a\bar{z} + \bar{w}$.

Teorema 1.11: $z = \bar{z}$ si y sólo si z es un número real.

Teorema 1.12: Para todo número natural $m \geq 2$ y todo número dual z, $\overline{z^m} = (\bar{z})^m$.

Demostración:
Por inducción sobre m. Se verifica para $m = 2$. Si $z = (a, b)$, como consecuencia inmediata del *teorema 1.9*, se tiene que $\overline{z^2} = (\bar{z})^2$.

Ahora se supone que se cumple para algún $m = k$; es decir que,

$$\overline{z^k} = (\bar{z})^k$$

Se debe probar que

$$\overline{z^{k+1}} = \left(\bar{z}\right)^{k+1}$$

Pero,

$$\overline{z^{k+1}} = \left(\overline{z^k \times z}\right)$$

por el *teorema 1.9*

$$= \left(\overline{z^k} \times \bar{z}\right)$$

por la hipótesis de inducción

$$= \left(\bar{z}^k \times \bar{z}\right)$$

y de acuerdo con la definición de potenciación con k un número natural.

$$= \left(\bar{z}\right)^{k+1}$$

Por lo tanto, la fórmula es válida para todo número natural m.

Definición 1.4: Un elemento (x, y) en D es una *unidad* o es *invertible* si existe un (w, t) en D tal que $(x, y)(w, t) = (1, 0)$, éste elemento (w, t) es único y es el inverso de (x, y) denotado también por $(x, y)^{-1}$.

Teorema 1.13: Las unidades en D son de la forma (a, b) con $a \neq 0$ y

$$(a, b)^{-1} = \frac{1}{a^2}(a, -b) = (a^{-1}, -ba^{-2}).$$

Teorema[5] *1.14**: El conjunto de las unidades $U(D)$, es un grupo abeliano con la operación de multiplicación de D.

[5] Este teorema se cumple en cualquier anillo conmutativo con identidad. De aquí en adelante este tipo de teoremas estarán marcados con *.

Teorema 1.15: $U(D)$ con la multiplicación estructura de *cuasigrupo*[6].

Demostración:

Las funciones

$$L_a: U(D) \to U(D) \quad \text{y} \quad R_a: U(D) \to U(D)$$
$$z \mapsto az \qquad\qquad z \mapsto za$$

son funciones biyectivas en $U(D)$; dicho de otra forma si para todo a y b en $U(D)$, las ecuaciones

$$az = b \qquad wa = b$$

tienen soluciones únicas[7].

1.2. DIVISIÓN ENTRE NÚMEROS DUALES

Definición 1.5: La división entre dos números duales $z = (a, b)$ y $w = (c, d)$ en $U(D)$, es:

$$\frac{z}{w} = zw^{-1}$$

y en términos de sus componentes:

$$z \times w^{-1} = (a,b) \times \frac{1}{c^2}(c,-d)$$

que se puede escribir como

$$z \times w^{-1} = \frac{(a,b)}{(c,d)} \times \frac{(c,-d)}{(c,-d)}.$$

[6] La definición de cuasigrupo se debe a B.A. HAUSMANN y O. ORE (HAUSMANN, B., ORE, O., *Theory of quasigroups,* Amer. J. Math. **59** (1937), 983 – 1004.), basados en el estudio de las estructuras no asociativas de R. MOUFANG (1905 – 1977) quién descubrió en 1937 la relación entre los planos proyectivos no–desarguesianos y esta estructura.

[7] Esta propiedad forma parte de los axiomas de Hilbert para los números reales en HILBERT, D. *Fundamentos de la Geometría*. Madrid, Publicaciones del Instituto Jorge Juan de Matemáticas. 1953. p.p. 244 – 249.

Teorema 1.16: $U(D)$ tiene estructura de *cuasigrupo* con la división.

1.3. LOS NÚMEROS DUALES COMO ESPACIO SEMINORMADO

Teorema 1.17: La función

$$\begin{aligned} \| \ \| : \quad D \quad &\to \quad R \\ z = (a, b) \ &\mapsto \ \| z \| = | a | \end{aligned}$$

define una *seminorma*[8] en D.

Demostración:

Se desprende de las propiedades del valor absoluto de los números reales que para todo z, w en D y c en R, se cumple que:

1. $\| z \| \geq 0$
2. $\| z \| = \| \bar{z} \|$
3. $\| z \bar{z} \| = \| z \|^2$
4. $\| zw \| = \| z \| \, \| w \|$
5. $\| z + w \| \leq \| z \| + \| w \|$
6. $\| cz \| = | c | \, \| z \|$

Para todo z un número dual nilpotente, se tiene que $\| z \| = 0$ aunque $z \neq 0$.

Teorema 1.18: La función

$$\begin{aligned} d: D \times D \quad &\to \qquad R^+ \cup \{0\} \\ (z, w) \quad &\mapsto \ d(z, w) = \| w - z \| = | c - a | \end{aligned}$$

donde $z = (a, b)$, $w = (c, d)$, define una *seudométrica* [9] en D.

[8] Rowland, Todd. "Seminorm." From *MathWorld* – A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/Seminorm.html

Demostración:

Se desprende de las propiedades del valor absoluto de los números reales que para todo z, w en D se cumple que:

1. $d(z, w) \geq 0$
2. $d(z, w) = d(w, z)$
3. $d(z, t) + d(t, w) \geq d(z, w)$.

Si dos números duales z y w tienen igual la primera componente, entonces $d(z, w) = 0$ aunque $z \neq w$.

1.4. OTRAS REPRESENTACIONES DE LOS NÚMEROS DUALES

1.4.1. Representación matricial

Un número dual puede representarse con una matriz 2×2 con entradas en R, mediante el homomorfismo inyectivo definido por

$$\delta: D \rightarrow M_{2\times 2}$$
$$(a,b) \mapsto \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$$

puesto que

$$\delta[(a, b) + (c, d)] = \delta[(a + c, b + d)]$$
$$= \begin{pmatrix} a+c & 0 \\ b+d & a+c \end{pmatrix}$$
$$= \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} + \begin{pmatrix} c & 0 \\ d & c \end{pmatrix}$$

[9] Barile, Margherita. "Pseudometric." From *MathWorld* – A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/Pseudometric.html

$$= \delta[(a, b)] + \delta[(c, d)]$$

y

$$\begin{aligned}\delta[(a, b)(c, d)] &= \delta[(ac, ad + bc)] \\ &= \begin{pmatrix} ac & 0 \\ ad + bc & ac \end{pmatrix} \\ &= \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}\begin{pmatrix} c & 0 \\ d & c \end{pmatrix} \\ &= \delta[(a, b)]\delta[(c, d)].\end{aligned}$$

Además es inyectiva ya que el núcleo de δ es igual al conjunto cuyo único elemento es 0.

1.4.2. Representación polar

También es posible representar un número dual utilizando un análogo a las coordenadas polares del plano complejo, definiendo la noción de circunferencia, ángulo y funciones trigonométricas duales.

Definición 1.6: Una *circunferencia dual* con centro en $z_0 = (a_0, b_0)$ y radio un número real r es el conjunto de puntos $z = (a, b)$, tales que

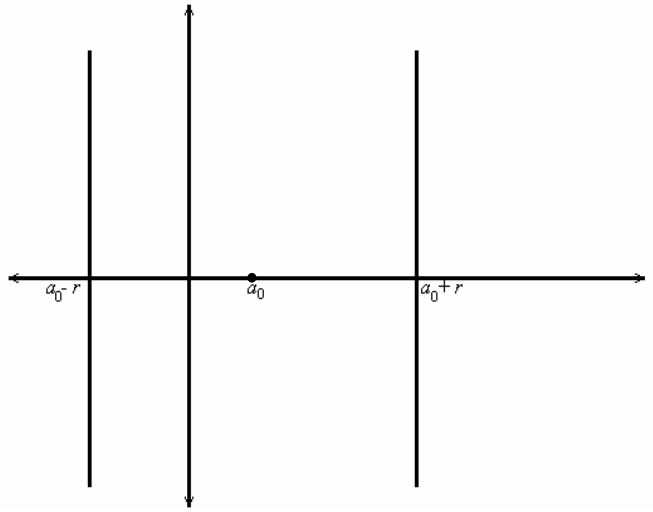
$$|| z - z_0 || = r$$

o sea

$$| a - a_0 | = r$$

cuya representación gráfica está dada por dos líneas verticales

$$a = a_0 + r \qquad \text{y} \qquad a = a_0 - r$$



Nótese que toda circunferencia tiene infinitos centros, porque todos los puntos sobre la vertical que contiene a z_0 están a la misma distancia r de los puntos sobre la circunferencia.

Si se piensa en un número dual $z = (a, b)$, no nilpotente, como un *segmento rectilíneo dirigido* o *vector*, desde el origen (0, 0) al punto (a, b), la *magnitud dual* [10] del vector es su seminorma $\| z \| = | a |$.

Definición 1.7: El *ángulo dual* θ entre el vector y la parte positiva del eje real, que se llamará también *argumento dual* del número es

$$\theta = \frac{b}{|a|}$$

A diferencia de los números complejos, el argumento dual de un número dual $z = (a, b)$ con $a \neq 0$, es único.

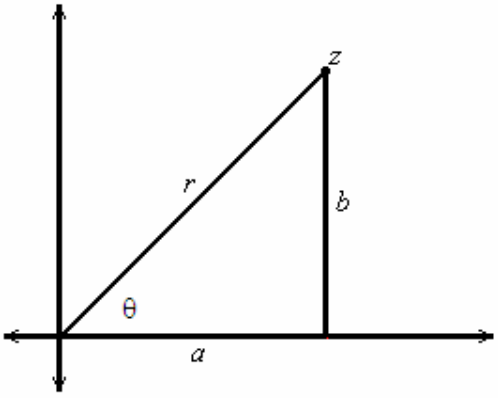
Definición 1.8: El *coseno dual* del *ángulo dual* θ es:

[10] La palabra *magnitud* no significa lo mismo que en geometría euclidiana, se usa por analogía.

$$cosd\ \theta = \frac{a}{|a|} = \begin{cases} 1 & \text{si } a > 0 \\ -1 & \text{si } a < 0 \end{cases}$$

Definición 1.9: El *seno dual* del *ángulo dual* θ es:

$$send\ \theta = \frac{b}{|a|} = \theta$$



Definición 1.10: La representación polar de un número dual $z = (a, b)$ no nilpotente es:

$$z = r\ (cosd\ \theta + n\ send\ \theta)$$

donde

$$r = |a|$$

y

$$a = r\ cosd\ \theta$$

$$b = r\ send\ \theta$$

z también puede escribirse como:

$$z = r e^{n\theta}$$

siempre que

$$e^{n\theta} = cosd\ \theta + n\ send\ \theta$$

esto es equivalente a:

$$e^{n\theta} = 1 + n\,\theta \qquad \text{si} \quad a > 0$$

$$e^{n\theta} = -1 + n\,\theta \qquad \text{si} \quad a < 0$$

Y finalmente, cualquier número dual no nilpotente se representa en forma polar como

$$z = r\,(cosd\,\theta + n\,send\,\theta)$$

o

$$z = (a, b) = r\,(1 + n\,\theta) \qquad \text{si } a > 0$$

$$z = (a, b) = r\,(-1 + n\,\theta) \quad \text{si } a < 0.$$

El significado geométrico de la multiplicación se obtiene de multiplicar

$$z = a + nb \quad \text{y} \quad w = c + nd$$

en forma polar, con los siguientes resultados

$$zw = r_1 r_2\,(1 + n\,(\theta_1 + \theta_2)) \quad \text{si } (a > 0 \text{ y } c > 0)$$

o

$$zw = r_1 r_2\,(1 - n\,(\theta_1 + \theta_2)) \quad \text{si } (a < 0 \text{ y } c < 0)$$

o

$$zw = r_1 r_2\,(-1 - n\,(\theta_1 - \theta_2)) \quad \text{si } (a > 0 \text{ y } c < 0)$$

o

$$zw = r_1 r_2\,(-1 + n\,(\theta_1 - \theta_2)) \quad \text{si } (a < 0 \text{ y } c > 0).$$

Un resultado análogo al resultado en los números complejos.

Como la magnitud dual del elemento idéntico de la multiplicación es 1 y su argumento es 0, entonces El inverso multiplicativo de un número dual no nilpotente

$$z = a + nb = r\,(1 + n\,\theta) \qquad \text{si } a > 0$$

$$z = a + nb = r\,(-1 + n\,\theta) \quad \text{si } a < 0$$

es

$$z^{-1} = \frac{1}{r}(1 - n\,\theta) \quad \text{si } a > 0$$

$$z^{-1} = \frac{1}{r}(-1 - n\,\theta) \quad \text{si } a < 0.$$

Y como el cociente, cuando existe, entre dos números duales $z = a + bn$ y $w = c + dn$ es el producto entre el primero y el inverso multiplicativo del segundo, entonces, si

$$z = r_1\,(1 + n\,\theta_1) \quad \text{cuando } a > 0$$

$$z = r_1\,(-1 + n\,\theta_1) \quad \text{cuando } a < 0$$

y

$$w = r_2\,(1 + n\,\theta_2) \quad \text{cuando } c > 0$$

$$w = r_2\,(-1 + n\,\theta_2) \quad \text{cuando } c < 0$$

se tiene que

$$\frac{z}{w} = \frac{r_1}{r_2}(1 + n\,(\theta_1 - \theta_2)) \quad \text{si } (a > 0 \text{ y } c > 0)$$

o

$$\frac{z}{w} = \frac{r_1}{r_2}(1 - n\,(\theta_1 - \theta_2)) \quad \text{si } (a < 0 \text{ y } c < 0)$$

o

$$\frac{z}{w} = \frac{r_1}{r_2}(-1 - n\,(\theta_1 + \theta_2)) \quad \text{si } (a > 0 \text{ y } c < 0)$$

o

$$\frac{z}{w} = \frac{r_1}{r_2}(-1 + n\,(\theta_1 + \theta_2)) \quad \text{si } (a < 0 \text{ y } c > 0)$$

En el caso en que z sea nilpotente no se le asigna una representación polar que tenga la misma forma que en el caso anterior pues tiene magnitud dual igual a 0.

1.5. POTENCIAS RACIONALES DE UN NÚMERO DUAL

Definición 1.11: Sea z un elemento de D y n un número natural, el elemento nz es:

Si $n = 0$

$$nz = (0, 0)$$

Si $n > 0$

$$(n + 1)z = nz + z$$

Definición 1.12: Sea z un elemento de D y n un número natural, el elemento z^n es:

Si $n = 0$

$$z^n = (1, 0)$$

Si $n > 0$

$$z^{n+1} = z^n z$$

Teorema 1.19:* Sea z, w elementos en D y m, n números naturales, se cumple que:

1. $m(z + w) = mz + mw$.
2. $(m + n)z = mz + nz$.
3. $m(nz) = (mn)z$.
4. $(zw)^m = z^m w^m$.
5. $z^{m+n} = z^m z^n$.
6. $(z^m)^n = z^{mn}$.

Teorema 1.20: Las potencias naturales de un número dual cualquiera $z = (a, b)$ están dadas por la fórmula[11]

[11] Un detalle curioso es que la primera componente sólo depende de a y en la segunda componente aparece la derivada de la primera componente, multiplicada por b. Para más información véase LUQUE, C. *El cálculo*

$$z^k = (a, b)^k = (a^k, ka^{k-1}b).$$

donde $k > 0$ es un número natural.

Demostración:

Se recurre a la inducción sobre k. Para iniciar se observa cuando $k = 1$:

$$z^1 = (a, b)^1 = (a, b)$$

y cuando $k = 2$:

$$z^2 = (a, b)^2 = (a, b)(a, b) = (a^2, 2ab).$$

Se supone que la afirmación se cumple para k:

$$z^k = (a, b)^k = (a^k, ka^{k-1}b)$$

y se debe demostrar que se cumple para $k + 1$:

$$z^{k+1} = (a, b)^{k+1}$$

por la *definición 1.12*

$$z^{k+1} = (a, b)^k (a, b)^1$$

aplicando la hipótesis de inducción y la *definición 1.12* se tiene que

$$z^{k+1} = (a^k, ka^{k-1}b)\ (a, b)$$

por la definición de multiplicación en los números duales y la propiedad distributiva de los números reales

$$z^{k+1} = (a^{k+1}, a^k b + ka^k b)$$

---

una versión sin el concepto de límite. En: Memorias VIII Coloquio Distrital de Matemáticas y Estadística. Bogotá, Universidad Pedagógica Nacional. 1991.

$$= (a^{k+1}, (n+1)a^k b).$$

En representación polar,

$$z = r\,(1 + n\theta) \quad \text{con} \quad a > 0$$

o

$$z = r\,(-1 + n\theta) \quad \text{con} \quad a < 0$$

entonces

$$z^k = r^k\,(1 + nk\theta) \quad \text{cuando} \quad a > 0$$

o

$$z^k = r^k\,((-1)^k + n(-1)^{k-1}\,k\,\theta) \quad \text{cuando} \quad a < 0.$$

Definición 1.13: Para todo entero positivo m, y todo z en D,

$$-mz = m(-z)$$

Definición 1.14: Para todo entero positivo m, y todo z en D no nilpotente

$$z^{-m} = (z^{-1})^m.$$

Definición 1.15: Dado $z = (a, b)$ no nilpotente, $w = (c, d)$ en D, si $w^k = z$ para cualquier número natural $k > 1$, w se llama una *raíz k-ésima* de z.

Teorema 1.21: Una raíz *k-ésima* de $z = (a, b)$ con $a > 0$, es:

$$w = r^{\frac{1}{k}}\left(1 + n\frac{\theta}{k}\right).$$

Demostración:

$$w^k = \left(r^{\frac{1}{k}}\left(1 + n\frac{\theta}{k}\right)\right)^k$$

Por el *teorema 1.19*

$$w^k = \left(r^{\frac{1}{k}}\right)^k \left(1 + \frac{n\theta}{k}\right)^k$$

Por la definición de potenciación en los números reales y el *teorema 1.20*

$$w^k = r\left(1^k + \frac{kn\theta}{k}\right)$$

$$w^k = r(1 + n\theta) = z.$$

Por tanto *w* es una *raíz k-ésima* de *z*, que se notará como $z^{\frac{1}{k}}$.

Teorema 1.22: Una raíz *k-ésima* de $z = (a, b)$ con $a < 0$ y *k* impar, es:

$$z^{\frac{1}{k}} = r^{\frac{1}{k}}\left(-1 + n\frac{\theta}{k}\right)$$

Demostración:

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}}\left(-1 + n\frac{\theta}{k}\right)\right)^k$$

Por el *teorema 1.19*

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}}\right)^k \left(-1 + \frac{n\theta}{k}\right)^k$$

Por la definición de potenciación en los números reales y el *teorema 1.20*

$$\left(z^{\frac{1}{k}}\right)^k = r\left((-1)^k + \frac{(-1)^{k-1} kn\theta}{k}\right)$$

$$\left(z^{\frac{1}{k}}\right)^k = r((-1)^k + (-1)^{k-1}\, n\theta)$$

y como k es impar, entonces

$$\left(z^{\frac{1}{k}} \right)^k = r(-1 + n\theta) = z.$$

Cuando k es par, z no tiene raíces k-ésimas, pues según lo anterior:

$$\left(z^{\frac{1}{k}} \right)^k = \left(r^{\frac{1}{k}} \left(-1 + n\frac{\theta}{k} \right) \right)^k$$

$$= r((-1)^k + (-1)^{k-1} n\theta)$$

y como k es par

$$= r(1 - n\theta) \neq z.$$

Si se quiere encontrar una estructura donde tenga solución el problema, se puede extender el anillo de los números duales de dos maneras naturales:

1.5.1. El anillo conmutativo con unidad de los números duales con coeficientes complejos

Definición 1.16: El conjunto

$$D[i] = \{(z, w) \mid z, w \in C\}$$

donde C es el conjunto de los números complejos, con la adición definida componente a componente y la multiplicación definida por

$$(z, w)(z', w') = (zz', zw' + wz')$$

se llama el conjunto de los números duales con coeficientes complejos.

Teorema 1.23: $D[i]$ es un anillo conmutativo con unidad ((1, 0), (0, 0)).

Teorema 1.24: $D[i]$ es representable como un conjunto de cuaternas ordenadas de números reales:

$$D[i] = \{(a, b, c, d) \mid a, b, c, d \in R\}$$

con adición y multiplicación definidas por:

$$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$$

$$(a, b, c, d)\,(a', b', c', d') = (aa' - bb', ab' + ba', ac' - bd' + ca' - db', ad' + bc' + cb' + da')$$

y con unidad (1, 0, 0, 0).

Teorema 1.25: $D[i]$ es representable como un conjunto

$$D[i] = \{(a + bi + cn + dk) \mid a, b, c, d \in R\}$$

con la adición definida por

$$(a + bi + cn + dk) + (a' + b'i + c'n + d'k) = (a + a') + (b + b')i + (c + c')n + (d + d')k$$

y la multiplicación cumple la propiedad distributiva y las siguientes igualdades:

$$i^2 = -1$$
$$n^2 = 0 = k^2$$
$$in = ni = k$$

Demostración:

Sea

$$1 = (1, 0, 0, 0) \qquad i = (0, 1, 0, 0) \qquad n = (0, 0, 1, 0) \qquad k = (0, 0, 0, 1)$$

con esto, cada cuaterna se escribe en la forma:

$$(a, b, c, d) = (a, 0, 0, 0)\ 1 + (b, 0, 0, 0)\ i\ + (c, 0, 0, 0)\ n + (d, 0, 0, 0)\ k$$

y como el subanillo

$$\{(t, 0, 0, 0) \mid t \in \mathrm{R}\}$$

es isomorfo con R, el elemento $(a, 0, 0, 0)$ se puede escribir como a.

Teorema 1.26: El conjunto de las cuaternas de la forma $(a, 0, c, 0) = a + cn$ forman un subanillo isomorfo con D.

Teorema 1.27: El conjunto de las cuaternas de la forma $(a, b, 0, 0) = a + bi$ forman un subanillo isomorfo con C.

1.5.2. El anillo conmutativo con unidad de los complejos con coeficientes duales

Definición 1.17: El conjunto

$$C[n] = \{(z, w) \mid z = (a, b), w = (c, d); z, w \in D\}$$

con la adición definida componente a componente y la multiplicación definida por

$$(z, w)(z', w') = (zz' - ww', zw' + wz')$$

se llama el conjunto de los números complejos con coeficientes duales.

Teorema 1.28: $C[n]$ es un anillo conmutativo con unidad $((1, 0), (0, 0))$.

Teorema 1.29: $C[n]$ es representable como un conjunto de cuaternas ordenadas de números reales:

$$C[n] = \{(a, b, c, d) \mid a, b, c, d \in R\}$$

con adición y multiplicación definidas por:

$$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$$

$$(a, b, c, d)(a', b', c', d') = (aa' - cc', ba' + ab' - dc' - cd', ac' + ca', ad' + bc' + cb' + da')$$

y con unidad (1, 0, 0, 0).

Teorema 1.30: $C[n]$ es representable como un conjunto

$$C[n] = \{(a + bn + ci + dk) \mid a, b, c, d \in R\}$$

con la adición definida por

$$(a + bn + ci + dk) + (a' + b'n + c'i + d'k) = (a + a') + (b + b')n + (c + c')i + (d + d')k$$

y la multiplicación cumple la propiedad distributiva y las siguientes igualdades:

$$i^2 = -1$$
$$n^2 = 0 = k^2$$
$$in = ni = k$$

Demostración:

Sea

$$1 = (1, 0, 0, 0) \qquad n = (0, 1, 0, 0) \qquad i = (0, 0, 1, 0) \qquad k = (0, 0, 0, 1)$$

con esto, cada cuaterna se escribe en la forma:

$$(a, b, c, d) = (a, 0, 0, 0)\ 1 + (b, 0, 0, 0)\ n\ + (c, 0, 0, 0)\ i + (d, 0, 0, 0)\ k$$

y como el subanillo

$$\{(t, 0, 0, 0) \mid t \in \mathrm{R}\}$$

es isomorfo con R, el elemento $(a, 0, 0, 0)$ se puede escribir como a.

Teorema 1.31: El conjunto de las cuaternas de la forma $(a, 0, c, 0) = a + ci$ forman un subanillo isomorfo con C.

Teorema 1.32: El conjunto de las cuaternas de la forma $(a, b, 0, 0) = a + bn$ forman un subanillo isomorfo con D.

Teorema 1.33: Los anillos $D[i]$ y $C[n]$ son isomorfos.

Demostración:
La función

$$\begin{aligned} f:\quad D[i] \quad &\to \quad C[n] \\ (a, b, c, d) \ &\mapsto f(a, b, c, d) = (a, c, b, d) \end{aligned}$$

Es un homomorfismo de anillos pues

$$\begin{aligned} f[(a, b, c, d) + (x, y, u, v)] &= f(a + x, b + y, c + u, d + v) \\ &= (a + x, c + u, b + y, d + v) \\ &= (a, c, b, d) + (x, u, y, v) \\ &= f(a, b, c, d) + f(x, y, u, v). \end{aligned}$$

y

$$\begin{aligned} f[(a, b, c, d)(x, y, u, v)] &= f(ax - by, ay + bx, au - bv + cx - dy, av + bu + cy + dx) \\ &= (ax - by, au - bv + cx - dy, ay + bx, av + bu + cy + dx) \end{aligned}$$

$$= (a, c, b, d)\,(x, u, y, v)$$
$$= f(a, b, c, d)\, f(x, y, u, v)$$

además es inyectiva pues el núcleo de f es igual al conjunto cuyo único elemento es 0 y es sobreyectiva.

Retomando el problema de hallar las raíces k-ésimas de un número dual, se puede escoger uno de los anillos anteriores, por ejemplo $D[i]$.

Teorema 1.34: Una raíz *k-ésima* de $z = (a, b)$ en $D[i]$ con $a < 0$ y k par de la forma $4t + 2$, es:

$$z^{\frac{1}{k}} = r^{\frac{1}{k}} i\left(1 - n\frac{\theta}{k}\right).$$

Demostración:

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}} i\left(1 - n\frac{\theta}{k}\right)\right)^k$$

Por la definición de potenciación en los números complejos y el *teorema 1.20*

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}}\right)^k i^k \left(1 - \frac{n\theta}{k}\right)^k$$

$$\left(z^{\frac{1}{k}}\right)^k = r i^k \left(1^k - \frac{kn\theta}{k}\right)$$

$$\left(z^{\frac{1}{k}}\right)^k = r i^k (1 - n\theta)$$

como k es de la forma $4t + 2$, entonces

$$i^k = -1$$

y por tanto

$$\left(z^{\frac{1}{k}}\right)^k = r(-1 + n\theta) = z.$$

Si w es una raíz cuadrada de z también lo es $-w$, pues en cualquier anillo se cumple que $(-w)^2 = w^2$.

Teorema 1.35: Si w es una raíz *k-ésima* de z en $D[i]$, entonces αw es una raíz de z, donde α es una raíz *k-ésima* de la unidad en C.

Teorema 1.36: Una raíz *k-ésima* de $z = (a, b)$ en $D[i]$ con $a < 0$ y k par de la forma $4t$, con t impar, es:

$$z^{\frac{1}{k}} = r^{\frac{1}{k}} \frac{\sqrt{2}}{2}(1+i)\left(1 - n\frac{\theta}{k}\right).$$

Demostración:

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}}\left(\frac{\sqrt{2}}{2}\right)(1+i)\left(1 - n\frac{\theta}{k}\right)\right)^k$$

$$\left(z^{\frac{1}{k}}\right)^k = r^{\frac{k}{k}}\left(\frac{\sqrt{2}}{2}\right)^k (1+i)^k \left(1 - n\frac{\theta}{k}\right)^k$$

y como

$$\left(\frac{\sqrt{2}}{2}\right)^k (1+i)^k = \left(\frac{\sqrt{2}}{2}\right)^k \left(\sqrt{2}\right)^k \left(cos\frac{k\pi}{4} + isen\frac{k\pi}{4}\right)$$

$$= cos\pi t + isen\pi t$$

$$= -1$$

entonces

$$\left(z^{\frac{1}{k}}\right)^k = -r\left(1 - \frac{kn\theta}{k}\right)$$

$$= r(-1 + n\theta) = z.$$

Teorema 1.37: Si z en $D[i]$ es nilpotente[12] $w^k = z$ para todo número natural $k > 1$, no tiene solución.

Demostración:
Se supone que existe w tal que $w^k = z$ con z nilpotente, entonces w debe ser nilpotente, porque si no lo fuera w^k no sería nilpotente, y esto contradice la hipótesis. Lo que significa que $w^k = 0$ para todo número natural $k > 1$ y esto también contradice la hipótesis. Por lo tanto no existe w que cumpla la condición.

Definición 1.18: Para todo número natural k y m, con $m \neq 0$, y todo z en D no nilpotente

$$z^{\frac{k}{m}} = \left(z^{\frac{1}{m}} \right)^k .$$

1.6. POTENCIAS DUALES DE UN NÚMERO DUAL

Definición 1.19: Para todo $z = (a, b)$ en D,

$$e^z = (e^a, e^a b).$$

Teorema 1.38: Para todo $z = (a, b)$ en D, $e^z \neq 0$.

Teorema 1.39: Para todo $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ en D, $e^{z_1} e^{z_2} = e^{z_1 + z_2}$.

Demostración:
Por la *definición 1.19* se tiene que

[12] En $D[i]$ los elementos nilpotentes son de la forma $(0, t)$ con 0 y t números complejos.

$$
\begin{aligned}
e^{z_1} e^{z_2} &= \left(e^{a_1}, e^{a_1} b_1\right)\left(e^{a_2}, e^{a_2} b_2\right) \\
&= \left(e^{a_1} e^{a_2}, e^{a_1} e^{a_2}\left(b_1 + b_2\right)\right) \\
&= \left(e^{a_1 + a_2}, e^{a_1 + a_2}\left(b_1 + b_2\right)\right) \\
&= e^{z_1 + z_2}
\end{aligned}
$$

Teorema 1.40: Para todo $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ en D, $\dfrac{e^{z_1}}{e^{z_2}} = e^{z_1 - z_2}$.

Teorema 1.41: Para todo $z = (a, b)$ en D y todo número natural k, $(e^z)^k = e^{zk}$.

Demostración:

Por la *definición 1.19*

$$(e^z)^k = (e^a, e^a b)^k$$

por el *teorema 1.20*

$$(e^z)^k = ((e^a)^k, k(e^a)^{k-1} e^a b)$$

$$(e^z)^k = (e^{ak}, e^{ak} bk)$$

y por la *definición 1.19*

$$(e^z)^k = e^{zk}.$$

Teorema 1.42: Para todo $z = (a, b)$ en D y todo número natural k, $(e^z)^{-k} = e^{-zk}$.

Demostración:

Por la *definición 1.14*

$$(e^z)^{-k} = ((e^z)^{-1})^k$$

Como $(e^z)^{-1} = \dfrac{1}{\left(e^a\right)^2}\left(e^a, -e^a b\right)$, entonces

$$(e^z)^{-k} = \left(\frac{1}{\left(e^a\right)^2}\left(e^a, -e^a b\right)\right)^k$$

y por los *teoremas 1.19* y *1.20*

$$(e^z)^{-k} = \left(\frac{1}{(e^a)^2}\right)^k \left((e^a)^k, -k(e^a)^{k-1} e^a b\right)$$

$$(e^z)^{-k} = \frac{1}{e^{2ak}}\left(e^{ak}, -k\, e^{ak} b\right)$$

$$(e^z)^{-k} = \left(e^{-ak}, -e^{-ak} bk\right)$$

$$(e^z)^{-k} = e^{-z\,k}.$$

Teorema 1.43: Para todo $z = (a, b)$ en D y todo número natural m, con $m \neq 0$, $\left(e^z\right)^{\frac{1}{m}} = e^{\frac{z}{m}}$.

Demostración:

Como $e^z = (e^a, e^a\, b)$

$$\left(e^z\right)^{\frac{1}{m}} = \left(e^a, e^a b\right)^{\frac{1}{m}}$$

por el *teorema 1.21*

$$\left(e^z\right)^{\frac{1}{m}} = \left(e^a\right)^{\frac{1}{m}} \left(1, \frac{e^a b}{m\, e^a}\right)$$

$$\left(e^z\right)^{\frac{1}{m}} = \left(e^{\frac{a}{m}}, e^{\frac{a}{m}} \frac{b}{m}\right)$$

$$\left(e^z\right)^{\frac{1}{m}} = e^{\frac{z}{m}}.$$

Teorema 1.44: Para todo $z = (a, b)$ en D, $e^{\bar{z}} = \overline{e^z}$.

Teorema 1.45: La función

$$f: D \to D^+ = \{(x, y) \in D : x > 0\}$$
$$z \mapsto f(z) = e^z$$

es biyectiva.

Demostración:

a) Dado $z = (a, b)$ y $w = (c, d)$ en D, si $e^z = e^w$ entonces $(e^a, e^a\, b) = (e^c, e^c\, d)$, por lo tanto $e^a = e^c$ de donde $a = c$ y $b = d$. Luego z = w, lo que prueba que f es inyectiva.

b) Dado $z = (a, b)$ con $a > 0$ existe $w = (c, d)$ en D, tal que $e^c = a$ y $e^c\, d = b$ con $c = ln\, a$ y $d = \frac{b}{a}$, lo que prueba que f es sobre.

La función inversa de f permite la siguiente

Definición 1.20: Dado $z = (a, b)$ en $D^+ = \{(x, y) \in D : x > 0\}$ y $w = (c, d)$ en D,

$$log\, z = w \text{ si y sólo si } e^w = z.$$

Teorema 1.46: Para todo $z = (a, b)$ en D^+, se cumple que

i. $e^{log\, z} = z$

ii. $log\,(e^z) = z$

Teorema 1.47: Para todo $z = (a, b)$ en D^+,

$$log\, z = \left(ln\, a,\ \frac{b}{a} \right).$$

Demostración:

Si $log\, z = w = (c, d)$ entonces $c = ln\, a$ y $d = \frac{b}{a}$ y por lo tanto

$$e^w = \left(e^{ln\, a}, e^{ln\, a}\, \frac{b}{a} \right) = (a, b) = z.$$

Teorema 1.48: Para todo z, w en D^+, $log(zw) = log\, z + log\, w$.

Demostración:

Dado $q = log\ z$ y $r = log\ w$ entonces por la *definición 1.20* $e^q = z$ y $e^r = w$, luego $zw = e^{q+r}$ y por tanto $q + r = log(zw)$.

Teorema 1.49: Para todo z, w en D^+, $log\left(\frac{z}{w}\right) = log\ z - log\ w$.

Teorema 1.50: Para todo z en D^+ y todo número natural n, $log(z^n) = n\ log\ z$.

Demostración:

Sea $z = (a, b)$ en D^+, por el *teorema 1.20*

$$\begin{aligned} log(z^n) &= log\ (a^n, na^{n-1}b\ ) \\ &= \left(ln\left(a^n\right), \frac{na^{n-1}b}{a^n} \right) \\ &= n\left(ln\, a, \frac{b}{a} \right) \\ &= n\ log\ z. \end{aligned}$$

Teorema 1.51: Para todo $z = (a, b)$ en D^+ y todo número natural n, $log\left(z^{\frac{1}{n}}\right) = \frac{1}{n} log\ z$.

Demostración:

Como $a > 0$, el *teorema 1.21* establece que

$$z^{\frac{1}{n}} = \left(a^{\frac{1}{n}}, \frac{a^{\frac{1}{n}}b}{na} \right)$$

luego

$$log\left(z^{\frac{1}{n}}\right) = log\left(a^{\frac{1}{n}}, \frac{a^{\frac{1}{n}}b}{na} \right)$$

$$log\left(z^{\frac{1}{n}}\right) = \left(ln\, a^{\frac{1}{n}}, \frac{a^{\frac{1}{n}} b}{na\; a^{\frac{1}{n}}}\right)$$

$$log\left(z^{\frac{1}{n}}\right) = \left(\frac{1}{n} ln\, a, \frac{b}{na}\right)$$

$$log\left(z^{\frac{1}{n}}\right) = \frac{1}{n} log\, z\,.$$

Teorema 1.52: Para todo $z = (a, b)$ en D^+, $log\,\bar{z} = \overline{log\, z}$.

Definición 1.21: Para todo z en D^+ y w en D,

$$z^w = e^{w\, logz}.$$

Teorema 1.53: Para todo z en D^+ y w, s en D, $z^{w+s} = z^w z^s$.

Demostración:

Por la *definición 1.21*

$$z^{w+s} = e^{(w+s)\, logz}$$

por la propiedad distributiva en D

$$z^{w+s} = e^{w\, logz + s\, logz}$$

por el *teorema 1.39*

$$z^{w+s} = e^{w\, logz}\; e^{s\, logz}$$

y por la *definición 1.21*

$$z^{w+s} = z^w z^s.$$

Teorema 1.54: Para todo z, v en D^+ y w en D, $(zv)^w = z^w v^w$.

Demostración:

Por la *definición 1.21*

$$(zv)^w = e^{w\ log(zv)}$$

por el *teorema 1.48*

$$(zv)^w = e^{w\ (logz\ +\ logv)}$$

por la propiedad distributiva en D y el *teorema 1.39*

$$(zv)^w = e^{w\ logz}\ e^{w\ logv}$$

y por la *definición 1.21*

$$(zv)^w = z^w\ v^w.$$

1.7. ECUACIONES EN LOS NÚMEROS DUALES

1.7.1. Ecuaciones de primer grado

Teorema 1.55: La ecuación $az + b = 0$ donde a y b están en D, $a^2 \neq 0$, tiene una *única* solución.

Demostración:
Si se parte de

$$az + b = 0$$

y se suma $(-b)$ a ambos lados de la igualdad, (estabilidad de la igualdad), se obtiene:

$$(az + b) + (-b) = 0 + (-b)$$

al usar las propiedades asociativa de la suma y del inverso aditivo, se llega a

$$az = -b$$

Ahora, como $a^2 \neq 0$ si se multiplica a ambos lados de la igualdad por $\frac{1}{a}$, se consigue,

$$\frac{1}{a}(az) = \frac{1}{a}(-b)$$

Y al aplicar las propiedades asociativa y del elemento idéntico de la multiplicación, se tiene que

$$z = \frac{-b}{a}$$

y ésta es la *única* solución para la ecuación planteada.

1.7.2. Una ecuación con dos incógnitas

Teorema 1.56: La ecuación $az + bw = c$ donde a, b y c están en D, $a^2 \neq 0$, $b^2 \neq 0$, tiene infinitas soluciones dadas por

$$w = \frac{c - az}{b}.$$

El resultado que se obtiene es, que para cada valor que se elija para z en los números duales, se consigue un valor para w, también dentro de los números duales, siempre que todas las operaciones que se hagan estén definidas; además, no se puede graficar en un solo plano, se *requieren dos planos duales uno para z y otro para w*, variando z como se quiera; por ejemplo, si se tiene la ecuación

$$(-2, 1)z + w = (1, 3)$$

entonces

$$w = (2, -1)z + (1, 3)$$

si notamos $z = (x, y)$

$$w = (2, -1)(x, y) + (1, 3)$$

$$w = (2x, 2y - x) + (1, 3)$$

$$w = (2x + 1, 2y - x + 3)$$

y si se elige z a lo largo de la recta

$$y = x + 3$$

sus imágenes estarán en la recta

$$w = (2x + 1, 2(x + 3) - x + 3)$$

$$w = (2x + 1, x + 9)$$

si notamos $w = (u, v)$

$$u = 2x + 1$$

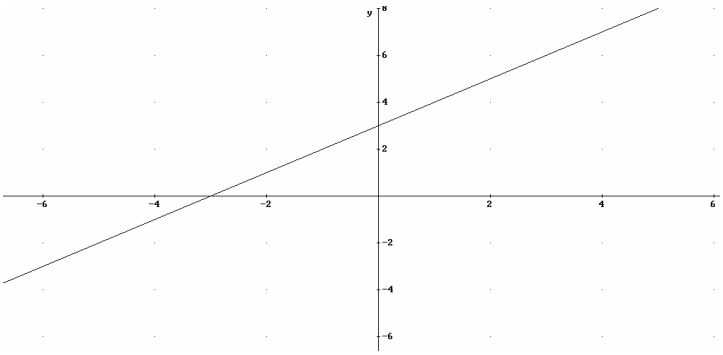
y

$$v = x + 9$$

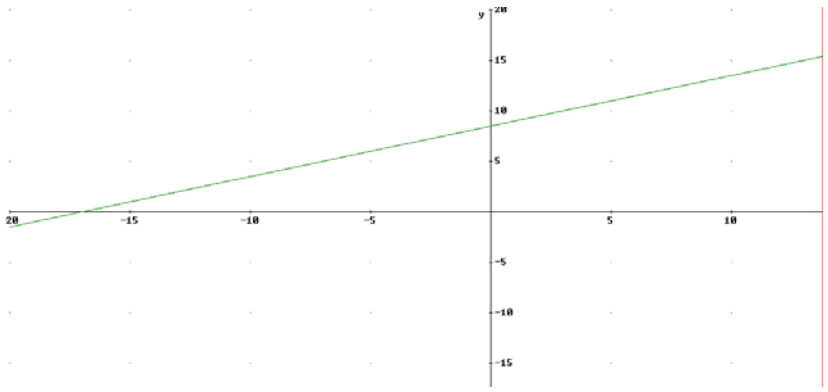
despejando x en términos de u y reemplazando en v se obtiene

$$v = \frac{u + 17}{2}$$

Entonces en el plano z se grafica la recta $y = x + 3$:



Y en el plano w se grafica la recta $v = \dfrac{u+17}{2}$:



1.7.3. Ecuaciones de segundo grado

Teorema 1.57: La ecuación $az^2 + bz + c = 0$ donde *a, b y c* están en $D[i]$ y si se cumple uno de los casos:

i. $a = (a_1, a_2)$, $b = (b_1, b_2)$, y $c = (c_1, c_2)$ son números no nilpotentes y $b_1^2 - 4a_1c_1 \neq 0$

ii. a, c son no nilpotentes y b nilpotente

iii. a, b son no nilpotentes y c nilpotente

tiene dos soluciones dadas por

$$z_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{y} \quad z_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Demostración:

i. Se parte de la ecuación $az^2 + bz + c = 0$ donde $a = (a_1, a_2)$, $b = (b_1, b_2)$, y $c = (c_1, c_2)$ son números no nilpotentes en $D[i]$ y $b_1^2 - 4a_1c_1 \neq 0$, luego para resolver la ecuación se suma $(-c)$ a ambos lados de la ecuación y se obtiene

$$(az^2 + bz + c) + (-c) = 0 + (-c)$$

$$az^2 + bz = (-c)$$

Como $a^2 \neq 0$, tiene inverso y se multiplica por $\frac{1}{a}$ a ambos lados de la ecuación para conseguir

$$\frac{1}{a}\left(az^2 + bz\right) = \frac{1}{a}\left(-c\right)$$

$$z^2 + \frac{b}{a}z = -\frac{c}{a}$$

Ahora se suma $\left(\frac{b}{2a}\right)^2$ a ambos lados de la ecuación, con el propósito de formar un cuadrado perfecto,

$$z^2 + \frac{b}{a}z + \left(\frac{b}{2a}\right)^2 = -\frac{c}{a} + \left(\frac{b}{2a}\right)^2$$

y como

$$z^2 + \frac{b}{a}z + \left(\frac{b}{2a}\right)^2 = \left(z + \frac{b}{2a}\right)^2$$

Al reemplazar en la ecuación, y al utilizar que $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, se obtiene que:

$$\left(z + \frac{b}{2a}\right)^2 = -\frac{c}{a} + \frac{b^2}{4a^2}$$

$$\left(z + \frac{b}{2a}\right)^2 = \frac{-4ac + b^2}{4a^2}$$

$$\left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

Y al sumar la expresión $\left(-\frac{b^2-4ac}{4a^2}\right)$ a ambos lados de la igualdad,

$$\left(z^2+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}=0$$

Como se tiene que

$$x^2-y^2=(x-y)(x+y),$$

$x^2 = t$ significa que $x=\sqrt{t}$, y la definición de radicación

$$\sqrt{4a^2}=2a$$

se consigue que,

$$\left(z+\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}\right)\left(z+\frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}\right)=0\,.$$

Como $b_1^2-4a_1c_1\neq 0$, $\left(b^2-4ac\right)^{\frac{1}{2}}$ existe y es no nilpotente, además puesto que $a_1\neq 0$, $c_1\neq 0$ entonces $a_1c_1\neq 0$ y $\left(b_1^2-4a_1c_1\right)^{\frac{1}{2}}\neq b_1$. Luego

$$\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}=u \quad \text{y} \quad \frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}=v$$

son no nilpotentes. Entonces para que se cumpla que

$$(z+u)(z+v)=0$$

debe darse que

$$z=-u \quad \text{y} \quad z=-v$$

o

$$z+u=h \quad \text{y} \quad z=-v$$

o

$$z = -u \quad \text{y} \quad z + v = j$$

o

$$z + u = l \quad \text{y} \quad z + v = m$$

donde h, j, l y m son elementos nilpotentes en $D[i]$.

Pero para que $-u + h$ sea una raíz de la ecuación $az^2 + bz + c = 0$ es necesario que

$$a(-u + h)^2 + b(-u + h) + c = 0$$
$$a(u^2 - 2uh + h^2) - bu + bh + c = 0$$

y como $au^2 - bu + c = 0$ y $h^2 = 0$ entonces

$$-2auh + bh = 0$$
$$h(-2au + b) = 0$$

y como u, a y b son no nilpotentes, $-2au + b$ es no nilpotente, luego $h = (0, 0)$.

Por tanto las soluciones de la ecuación $az^2 + bz + c = 0$ se reducen a

$$z_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{y} \quad z_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

ii. Se parte de la ecuación $az^2 + bz + c = 0$ donde $a = (a_1, a_2)$, $c = (c_1, c_2)$ son números no nilpotentes y $b = (0, b_2)$ es nilpotente en $D[i]$, luego para resolver la ecuación se realiza el procedimiento anterior hasta obtener que

$$\left(z + \frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a} \right) \left(z + \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a} \right) = 0.$$

Como $b^2 = 0$ y $a_1 \neq 0$, $c_1 \neq 0$ entonces $b^2 - 4ac \neq 0$, por tanto $\left(b^2 - 4ac\right)^{\frac{1}{2}}$ existe y es no nilpotente. Luego

$$\frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a} = u \quad \text{y} \quad \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a} = v$$

son no nilpotentes. Entonces para que se cumpla que

$$(z + u)(z + v) = 0$$

debe darse que

$$z = -u \quad \text{y} \quad z = -v$$

o

$$z + u = h \quad \text{y} \quad z = -v$$

o

$$z = -u \quad \text{y} \quad z + v = j$$

o

$$z + u = l \quad \text{y} \quad z + v = m$$

donde h, j, l y m son elementos nilpotentes en $D[i]$.

Y por la misma razón presentada en el caso anterior, las soluciones de la ecuación $az^2 + bz + c = 0$ se reducen a

$$z_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{y} \quad z_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

iii. Se parte de la ecuación $az^2 + bz + c = 0$ donde $a = (a_1, a_2)$, $b = (b_1, b_2)$ son números no nilpotentes y $c = (0, c_2)$ es nilpotente en $D[i]$, luego para resolver la ecuación se realiza el procedimiento anterior hasta obtener que

$$\left(z+\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}\right)\left(z+\frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}\right)=0\,.$$

Como $c_1 = 0$, entonces $b_1^2 - 4a_1c_1 = b_1^2 \neq 0$, por tanto $\left(b^2-4ac\right)^{\frac{1}{2}}$ existe y es no nilpotente. Luego

$$\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}=u$$

es nilpotente y

$$\frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}=v$$

es no nilpotente. Entonces para que se cumpla que

$$(z+u)(z+v)=0$$

debe darse que

$$z=-u \quad \text{y} \quad z=-v$$

o

$$z+u=h \quad \text{y} \quad z=-v$$

o

$$z=-u \quad \text{y} \quad z+v=j$$

o

$$z+u=l \quad \text{y} \quad z+v=m$$

donde h, j, l y m son elementos nilpotentes en $D[i]$.

Pero para que $-u + h$ sea una raíz de la ecuación $az^2 + bz + c = 0$ es necesario que

$$a(-u+h)^2+b(-u+h)+c=0$$
$$a(u^2-2uh+h^2)-bu+bh+c=0$$

y como $au^2 - bu + c = 0$ y $h^2 = 0$ entonces

$$-2auh + bh = 0$$
$$h(-2au + b) = 0$$

y puesto que u es nilpotente, $-2au$ es nilpotente, pero como b es no nilpotente, $-2au + b$ es no nilpotente, luego $h = (0, 0)$.

Por tanto las soluciones de la ecuación $az^2 + bz + c = 0$ se reducen a

$$z_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{y} \quad z_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Ejemplo

1. La ecuación

$$(2, 3)z^2 + (1, 2)z + (0, 1) = 0$$

tiene por soluciones

$$z = \frac{(-1, -2) \pm \sqrt{(1, 2)^2 - 4(2, 3)(0, 1)}}{2(2, 3)}$$

$$z = \frac{(-1, -2) \pm \sqrt{(1, -4)}}{(4, 6)}$$

$$z = \frac{(-1, -2) \pm (1, -2)}{(4, 6)}$$

lo que significa que las dos raíces son:

$$z_1 = \frac{(-1, -2) + (1, -2)}{(4, 6)} = \frac{(0, -4)}{(4, 6)} = (0, -4)\left(\frac{1}{4}, -\frac{3}{8}\right) = (0, -1)$$

$$z_2 = \frac{(-1,-2)-(1,-2)}{(4,6)} = \frac{(-2,0)}{(4,6)} = (-2,0)\left(\frac{1}{4},-\frac{3}{8}\right) = \left(-\frac{1}{2},\frac{3}{4}\right).$$

1.8. CUATERNIOS DUALES

Definición 1.22: El conjunto

$$H_D = \{(a, b, c, d) \mid a, b, c, d \in R\}$$

donde R es el conjunto de los números reales, con la adición y multiplicación definidas por:

$$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$$

$$(a, b, c, d)\,(a', b', c', d') = (aa', ab' + ba', ac' + ca', ad' + bc' - cb' + da')$$

se llama el conjunto de los números cuaternios duales.

Teorema 1.58: H_D es un anillo conmutativo con unidad[13] (1, 0, 0, 0).

Teorema 1.59: H_D es representable como un conjunto

$$H_D = \{(a + bn + cm + dk) \mid a, b, c, d \in R\}$$

con la adición definida por

$$(a + bn + cm + dk) + (a' + b'n + c'm + d'k)$$
$$= (a + a') + (b + b')n + (c + c')m + (d + d')k$$

Y la multiplicación cumple la propiedad distributiva y las siguientes igualdades:

[13] Realmente forma un *álgebra de Grassmann* pues, junto con su estructura de espacio vectorial, sus elementos generadores: *n, m* y *s* anticonmutan. (LUQUE, C., DUQUE, O. *Introducción a las Álgebras de Grassmann*. En las memorias del VII Encuentro de Geometría y sus Aplicaciones. 1996. pp. 227-252).

$$n^2 = m^2 = k^2 = 0$$

$$k = nm = -mn$$

es definida por

$$(a + bn + cm + dk)\,(a' + b'n + c'm + d'k\,)$$
$$= (aa') + (ab' + ba')n + (ac' + ca')m + (ad' + bc' - cb' + da')k.$$

Demostración:

Sea

$$1 = (1, 0, 0, 0) \qquad n = (0, 1, 0, 0) \qquad m = (0, 0, 1, 0) \qquad k = (0, 0, 0, 1)$$

con esto, cada cuaterna se escribe en la forma:

$$(a, b, c, d) = (a, 0, 0, 0)\,1 + (b, 0, 0, 0)\,n + (c, 0, 0, 0)\,m + (d, 0, 0, 0)\,k$$

y como el subanillo

$$\{(t, 0, 0, 0) \mid t \in \mathrm{R}\}$$

es isomorfo con R, el elemento $(a, 0, 0, 0)$ se puede escribir como a, luego

$$(a, b, c, d) = a + bn + cm + dk.$$

El conjunto de los números cuaternios duales con la adición y la multiplicación *no forman un dominio de integridad*, debido a la existencia de elementos divisores de cero, que corresponden a elementos de la forma $(0, b, c, d)$ para cualquier número real b, c y d.

Teorema 1.60: El elemento inverso multiplicativo de $q = a + bn + cm + dk$, con $a \neq 0$ es

$$q^{-1} = \frac{\bar{q}}{\|q\|^2} = \frac{1}{\|q\|^2}\left(a - bn - cm - dk\right)$$

donde se ha definido

$$\bar{q} = a - bn - cm - dk \quad y \quad \|q\|^2 = q\,\bar{q} = a^2.$$

Teorema 1.61: H_D es representable como un conjunto de matrices 4 ×4 con entradas en R

$$H_D = \left\{ \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} : a, b, c, d \in R \right\}$$

con la adición y multiplicación usual de matrices.

Demostración:

Se define la función

$$\delta : H_D \rightarrow \mathrm{M}_{4\times 4}$$

$$(a, b, c, d) \mapsto \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix}$$

que es un homomorfismo inyectivo puesto que

$$\delta[(a, b, c, d) + (a', b', c', d')] = \delta[(a + a', b + b', c + c', d + d')]$$

$$= \begin{pmatrix} a+a' & 0 & 0 & 0 \\ c+c' & a+a' & 0 & 0 \\ b+b' & 0 & a+a' & 0 \\ d+d' & b+b' & -(c+c') & a+a' \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} + \begin{pmatrix} a' & 0 & 0 & 0 \\ c' & a' & 0 & 0 \\ b' & 0 & a' & 0 \\ d' & b' & -c' & a' \end{pmatrix}$$

$$= \delta[(a, b, c, d)] + \delta[(a', b', c', d')]$$

$$\delta[(a, b, c, d)\,(a', b', c', d')] = \delta[(aa', ab' + ba', ac' + ca', ad' + bc' - cb' + da')]$$

$$= \begin{pmatrix} aa' & 0 & 0 & 0 \\ ac' + ca' & aa' & 0 & 0 \\ ab' + ba' & 0 & aa' & 0 \\ ad' + da' + bc' - cb' & ab' + ba' & -(ac' + ca') & aa' \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} \begin{pmatrix} a' & 0 & 0 & 0 \\ c' & a' & 0 & 0 \\ b' & 0 & a' & 0 \\ d' & b' & -c' & a' \end{pmatrix}$$

$$= \delta[(a, b, c, d)]\ \delta[(a', b', c', d')].$$

Además es inyectiva ya que el núcleo de δ es igual al conjunto cuyo único elemento es 0.

1.9. PREORDEN EN LOS NÚMEROS DUALES

Teorema 1.62: En los números duales no existe un conjunto de números positivos P.

Demostración:
Si existiera un conjunto de números positivos P, entonces debe cumplirse que:
Si $n \neq 0$, entonces $n \in$ P o $-n \in$ P.

Pero, si $n \in$ P entonces $n^2 = 0$ debe pertenecer a P y $0 \notin$ P. Y si $-n \in$ P, entonces $(-n)^2 = 0$ debe pertenecer a P y $0 \notin$ P.

Definición 1.23: Un subconjunto H de D se llamará de números D-Positivos si se cumple:

1. Si a y b pertenecen a H entonces $a + b$ y ab pertenecen a H.
2. Si a es un número dual, se cumple exactamente una de las tres situaciones:

$$a \in H, a^2 = 0, -a \in H$$

Definición 1.24: Para todo a, b en D,

$$a < b \text{ si y solo si } b - a \in H.$$
$$a > b \text{ si y solo si } b < a$$
$$a \leq b \text{ si y solo si } a < b \text{ o } a = b$$
$$a \geq b \text{ si y solo si } a > b \text{ o } a = b$$

Si $a < 0$ se dice que a es D-Negativo.

Teorema 1.63: La relación $<$ es transitiva.

Demostración:
Para todo a, b en D, si $a < b$ y $b < c$ entonces $b - a \in H$ y $c - b \in H$, por tanto su suma $(b - a) + (c - b) \in H$, es decir $c - a \in H$, luego $a < c$.

Teorema 1.64: La relación $\leq$ es un *preorden*[14] sobre D.

Dos números sobre la misma fibra vertical; es decir, con la primera componente igual, no son comparables.

La relación de preorden $\leq$, permite definir una relación de equivalencia sobre D, cuyas clases son las fibras verticales, es decir, los elementos que no son comparables:

[14] Clarkson, Michael. "Preorder." From *MathWorld* – A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/Preorder.html

$a \sim b$ si y sólo si a y b tienen la misma primera componente.

Si a y b son números duales, se cumple exactamente una de las siguientes condiciones:

$$a < b,\ a \sim b,\ b < a$$

Esto se debe a que el número $b - a$ está en una sola de las situaciones:

$$b - a > 0,\ \text{ó}\ (b-a)^2 = 0,\ \text{ó}\ b - a < 0$$

Teorema 1.65 (*Monotonía de la adición*): Dados números duales cualesquiera $x, y, z,$ y w si $x < y$ y $z < w$ entonces[15]:

$$x + z < y + w.$$

Demostración:

Si se supone que $x < y$ y $z < w$ entonces $(y - x) \in H$ y $(w - z) \in H$ y su suma

$$(y - x) + (w - z) \in H$$

pero esta suma puede escribirse como

$$(y + w) - (x + z) \in H$$

lo que significa que

$$x + z < y + w.$$

Teorema 1.66 (*Monotonía de la multiplicación*): Para todo x, y en D y z en H, si $x < y$ entonces $xz < yz$.

Demostración:

[15]A pesar de que no todo par de elementos son comparables, si x e y son comparables y z y w también, entonces $x + z$ es comparable con $y + w$.

Si se supone que $x < y$ entonces $(y - x) \in H$. Como z está en H, $z(y - x) \in H$, esto es $(zy - zx) \in H$, lo que significa que $xz < yz$.

Teorema: Para todo x, y en D y z es D-Negativo, si $x < y$, entonces $xz > yz$.

Teorema 1.67: Para todo x, y, z en D, si $x + z < y + z$ entonces $x < y$.

Un ejemplo de un conjunto de números D-Positivos para los números duales es el conjunto:

$$H = \{(x, y) \in D: x > 0\}.$$

1.10. SUBANILLOS DE LOS NÚMEROS DUALES

Teorema 1.68: Los siguientes subconjuntos de D son subanillos propios:

i. $S_1 = \{(0, b) \in D: b \in R\}$ es un anillo conmutativo con elementos nilpotentes.
ii. $S_2 = \{(a, 0) \in D: a \in R\}$ es un dominio de integridad isomorfo con R.
iii. $S_3 = \{(a, b) \in D: a, b \in Q\}$ es un anillo conmutativo con unidad y con elementos nilpotentes.
iv. $S_4 = \{(a, b) \in D: a, b \in Z\}$ es un anillo conmutativo con unidad y con elementos nilpotentes.
v. $S_5 = \{(0, b) \in D: b \in Q\}$ es un anillo conmutativo con elementos nilpotentes.
vi. $S_6 = \{(0, b) \in D: b \in Z\}$ es un anillo conmutativo con elementos nilpotentes.
vii. $S_7 = \{(a, 0) \in D: a \in Q\}$ es un dominio de integridad isomorfo con Q.
viii. $S_8 = \{(a, 0) \in D: a \in Z\}$ es un dominio de integridad isomorfo con Z.

1.11. IDEALES DE LOS NÚMEROS DUALES

Teorema 1.69: Sea $(0, b)$ en D, el conjunto de todos los elementos nilpotentes

$$\langle(0, b)\rangle = \{x\,(0, b) : x \in D\}$$

es un *ideal principal* en D.

Demostración:
Si $(0, i), (0, j) \in \langle(0, b)\rangle$ entonces

$$(0, i) - (0, j) = (0, i - j) \in \langle(0, b)\rangle.$$

Y si $(a, c) \in D$ y $(0, j) \in \langle(0, b)\rangle$ entonces

$$(a, c)(0, j) = (0, aj) \in \langle(0, b)\rangle.$$

Al ideal $\langle(0, b)\rangle$ se le llamará N.

Teorema 1.70: El ideal anulador de N es N.

Teorema 1.71: Si (x, y) es no nilpotente en D, entonces

$$\langle(x, y)\rangle = \{(z, w)(x, y) : (z, w) \in D\} = D.$$

El anillo D tiene sólo tres ideales que son $\{0\}$, D y N.

Definición 1.25: Un *ideal maximal* en D es un ideal propio M que no está contenido en un ideal propio estrictamente mayor.

Teorema 1.72: M* es un ideal maximal de *D* si, y sólo si $M \neq D$ e $\langle M, a\rangle = D$ para todo *a* que no está en *M*.

Demostración:
Se supone que *M* es un ideal maximal del anillo *D* y *a* un elemento que no pertenece a *M*. Si $\langle M, a\rangle$ es el ideal generado por el conjunto $M \cup \{a\}$, se cumple que $M \subset \langle M, a\rangle \subseteq D$. Estas inclusiones implican que si *M* es ideal maximal, $\langle M, a\rangle = D$.

Ahora se supone que *I* es un ideal en *D* tal que $M \subset I \subseteq D$, y si *a* es un elemento de *I* que no está en *M*, entonces $M \subset \langle M, a\rangle \subseteq I$. Pero como $\langle M, a\rangle = D$ entonces $I = D$ y con esto se concluye que *M* es un ideal maximal de *D*.

Teorema 1.73: M* es un ideal maximal en *D* si y sólo si D/M es un campo.

Demostración:
Se supone que *M* es un ideal maximal del anillo *D*, y como D/M es un anillo conmutativo con identidad, se necesita encontrar el inverso multiplicativo de un elemento $a + M$ de D/M, donde $a + M$ es distinto del elemento cero, es decir *a* no está en *M*.

Como *M* es maximal, entonces por el *teorema 1.72* se tiene que $\langle M, a\rangle = D$ para todo *a* que no está en *M*:

$$D = \langle M, a\rangle = \{ m + xa \mid m \in M, x \in D\}.$$

Como 1 está en *D*, se puede escribir de la forma

$$1 = m' + x'a$$

para determinados *m'* en *M* y *x'* en *D*, luego $1 - x'a$ está en *M*, es decir

$$1 + M = x'a + M = (x' + M)\,(a + M)$$

Con lo que se demuestra que $x' + M$ es el inverso multiplicativo de $a + M$.

Ahora se supone que D/M es un campo y que I es un ideal en D tal que $M \subset I \subseteq D$. Como M es un subconjunto propio de I existe a un elemento de I que no está en M, entonces $a + M$ tiene inverso multiplicativo

$$(a + M)\,(x + M) = 1$$

para $x + M$ en D/M . Entonces $1 - ax$ está en $M \subset I$ y como ax está en I pues es un ideal, la suma está en I, es decir, 1 está en I, luego $I = D$. Con lo que se demuestra que M es un ideal maximal en D.

Teorema 1.74: El ideal N es un ideal maximal en D.

Teorema 1.75: D/N es isomorfo con R.

Demostración:
Se define la función

$$\begin{aligned} \varphi:\ D/N &\rightarrow R \\ (a, b) + N &\mapsto a \end{aligned}$$

que es un homomorfismo puesto que

$$\begin{aligned} \varphi[((a, b) + N) + ((c, d) + N)] &= \varphi[(a + c, b + d) + N] \\ &= a + c \\ &= \varphi[((a, b) + N)] + \varphi[((c, d) + N)] \end{aligned}$$

$$\varphi[((a, b) + N)\,((c, d) + N)] = \varphi[(ac, ad + bc) + N]$$
$$= ac$$
$$= \varphi[((a, b) + N)]\,\varphi[((c, d) + N)]$$

Además φ es inyectiva pues $N_\varphi = \{N\}$ y φ es sobreyectiva pues dado a en R, existe $(x + y) + N$ en D/N tal que $x = a$ e y es cualesquier número real.

Definición 1.26: Un *ideal primo* en D es un ideal propio J tal que para todo z y w en D se tiene que si zw está en J entonces z está en J o w está en J.

Teorema 1.76: J* es un ideal primo en D si y sólo si D/J es un dominio de integridad.

Demostración:
Se supone que J es un ideal primo del anillo D, y como D/J es un anillo conmutativo con identidad, se necesita demostrar que no tiene divisores de cero.

Dados $z + J$ y $w + J$ en D/J, si $(z + J)(w + J) = 0 + J$ entonces $zw + J = 0 + J$ lo que significa que $zw - 0 = zw$ está en J, y como J es un ideal primo, entonces z está en J o w está en J, luego uno de los factores es el elemento cero J en D/J.
Ahora se supone que D/J es un dominio de integridad, luego si zw está en J, entonces $(z + J)(w + J)$ es el elemento cero J en D/J, siempre que $z + J = J$ o $w + J = J$, es decir, z está en J o w está en J.

Teorema 1.77: El ideal N es un ideal primo en D.

CAPÍTULO 2

EL ANILLO DE POLINOMIOS D[Z]

2.1. EL ANILLO DE LAS SERIES FORMALES DE POTENCIAS SUC(D)

Definición 2.1: Sea Suc(D) el conjunto de todas las sucesiones infinitas que se pueden formar con elementos de D, luego un elemento de Suc(D) es de la forma:

$$q = (a_0, a_1, a_2, \ldots, a_k, \ldots)$$

con a_k en D.

Definición 2.2: Dos elementos $p = (a_0, a_1, a_2, \ldots, a_k, \ldots)$ y $q = (b_0, b_1, b_2, \ldots, b_k, \ldots)$ de Suc(D) son iguales si y sólo si $a_k = b_k$ para todo $k \geq 0$.

Definición 2.3: En Suc(D) se definen dos operaciones, adición y multiplicación[16], como:

$$p + q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k, \ldots)$$

$$pq = (c_0, c_1, c_2, \ldots, c_k, \ldots)$$

para todo $k \geq 0$, en el cual cada c_k está dado por:

[16] No significa lo mismo que en Z, Q, R.

$$c_k = \sum_{i+j=k} a_i b_j = a_0 b_k, a_1 b_{k-1}, a_2 b_{k-2}, \ldots, a_k b_0 \quad \text{donde } i, j \geq 0.$$

*Teorema 2.1**: Con estas dos operaciones Suc(D) es un *anillo conmutativo con unidad*.

La sucesión con todos sus elementos iguales a 0, (0, 0, 0, …), es el elemento idéntico para la adición, la sucesión (1, 0, 0, 0, …) es el elemento idéntico para la multiplicación y el inverso aditivo de un elemento $p = (a_0, a_1, a_2, \ldots, a_k, \ldots)$ de Suc(D) es $-p = (-a_0, -a_1, -a_2, \ldots, -a_k, \ldots)$.

*Teorema 2.2**: En el anillo Suc(D) de las sucesiones con coeficientes en D, el conjunto

$$F = \{(a, 0, 0, ...) \mid a \in D\}$$

con la suma y multiplicación de las sucesiones es un subanillo de Suc(D).

Teorema 2.3: F es isomorfo con D.

Demostración:
La función

$$f : D \to F$$

tal que a cada elemento a de D se le asigna $f(a) = (a, 0, 0, 0, \ldots)$, es biyectiva y se cumple que:

$$f(a + b) = f(a) + f(b)$$

$$f(ab) = f(a) f(b).$$

Los elementos de D considerados como sucesiones se llaman *constantes*.

En Suc(D) se utiliza el símbolo Z para distinguir el elemento

$$Z = (0, 1, 0, 0, 0, ...)$$

que tiene un comportamiento particular: si se multiplica por él mismo, se obtiene:

$$Z^2 = Z \cdot Z = (0, 0, 1, 0, 0, ...)$$

si se insiste, resulta

$$Z^3 = Z \cdot Z \cdot Z = (0, 0, 0, 1, 0, 0, ...)$$

y así sucesivamente

$$Z^n = Z \cdot Z \cdot Z = (0, 0, 0, ... 1, ...0, 0, ...)$$

donde 1 está en la posición $n + 1$.

Con este resultado se puede escribir una sucesión cualquiera

$$t = (a_0, a_1, a_2, ..., a_i, ...)$$

como

$$t = (a_0, 0, 0, ...) + (0, a_1, 0, 0, ...) + (0, 0, a_2, 0, 0, ...) + \ldots + (0, 0, ..., a_i, 0, 0, ...) + \ldots$$

o lo que es igual

$$t = a_0(1, 0, 0, ...) + a_1(0, 1, 0, 0, ...) + a_2(0, 0, 1, 0, 0, ...) + ... + a_i (0, 0, ..., 1, 0, 0, ...) + ...$$

o sea que cualquier elemento del anillo Suc(D) se puede escribir como

$$t = a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots + a_i Z^i + ...$$

expresión que se denomina *serie formal de potencias sobre D* y a los elementos a_0, a_1, ..., a_i *coeficientes* de *t*. Otra forma de escribir la serie es:

$$t = t(Z) = \sum a_j Z^j$$

El elemento *Z* es usualmente llamado *indeterminada*. El anillo Suc(*D*) también recibe el nombre de *D*[[*Z*]].

2.2. EL ANILLO DE POLINOMIOS D[Z]

Definición 2.4: El conjunto de todas las series formales de *D*[[*Z*]] para las que existe un número natural *n*, con $n \geq 0$ tal que para todo número natural *k*, $k > n$, se tiene que $a_k = 0$ se denota como *D*[*Z*]. Entonces

$$D[Z] = \{ a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots + a_n Z^n : a_i \in D, n \geq 0 \}$$

Un elemento de *D*[*Z*] se llama polinomio con coeficientes en *D*.

Definición 2.5: Los polinomios $q(Z) = a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots + a_n Z^n$ y $g(Z) = b_0 + b_1 Z + b_2 Z^2 + b_3 Z^3 + \cdots + b_k Z^k$ en *D*[*Z*], son iguales si y solo si $a_i = b_i$ para todo valor de $i \geq 0$.

El mayor valor de *i* para el cual a_i no es cero, es llamado *grado del polinomio*.

2.2.1. Adición de polinomios

Definición 2.6: La suma de dos polinomios en *D*[*Z*], se define componente a componente.

Si

$$q(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n \quad \text{y} \quad g(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_k Z^k$$

Entonces

$$q(Z) + g(Z) = c_0 + c_1 Z + c_2 Z^2 + \ldots + c_m Z^m$$

donde

$$c_i = a_i + b_i \quad \text{para todo valor de } i \geq 0.$$

O sea que

$$q(Z) + g(Z) = (a_0 + b_0) + (a_1 + b_1) Z + (a_2 + b_2) Z^2 + \ldots + (a_m + b_m) Z^m$$

donde $m \leq máx\{n, k\}$.

El elemento idéntico[17] para la suma es

$$\mathbf{0} = (0, 0) + (0, 0) Z + (0, 0) Z^2 + \cdots + (0, 0) Z^j + (0, 0) Z^{j+1} + \ldots$$

El inverso aditivo de

$$q(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$$

en $D[Z]$, es

$$-q(Z) = -a_0 - a_1 Z - a_2 Z^2 - \cdots - a_n Z^n .$$

2.2.2. Multiplicación de polinomios

Definición 2.7: La multiplicación de

$$q(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n \quad \text{y} \quad g(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_k Z^k$$

en $D[Z]$, es

$$q(Z)\, g(Z) = c_0 + c_1 Z + c_2 Z^2 + \cdots + c_q Z^q$$

[17] Como de costumbre, se usa el símbolo 0, con significados análogos pero diferentes.

en el que cada

$$c_p = \sum_{k=0}^{p} a_k b_{p-k}$$

y $q \leq n + k$, donde q es el grado de $p(Z)\ q(Z)$, n es el grado del polinomio $q(Z)$ y k es el grado de $g(Z)$.

A diferencia de lo que ocurre en los dominios de integridad, en $D[Z]$ no se tiene la igualdad debido a la existencia de elementos nilpotentes en D, pues si dados dos polinomios cada uno con coeficientes principales nilpotentes, el grado del producto será menor que la suma de los grados de cada uno.

Ejemplo:

Al multiplicar $p(Z) = (2, 1) + (0, 1)Z$ y $q(Z) = (1, 2) + (0, 2)Z$ se tiene que

$$\begin{aligned} p(Z)\ q(Z) &= (2, 5) + (0, 4)Z + (0, 1)Z + (0, 0)Z^2 \\ &= (2, 5) + (0, 5)Z \end{aligned}$$

Donde el grado($p(Z)\ q(Z)$) < grado($p(Z)$) + grado($q(Z)$).

La igualdad se da cuando alguno de los dos polinomios tiene el coeficiente principal no nilpotente.

Ejemplo:

Si se multiplica $p(Z) = (0, 3) + (0, 2)Z + (2, 1)Z^2$ y $q(Z) = (1, 4) + (0, 1)Z$ se obtiene que

$$p(Z)\ q(Z) = (0, 3) + (0, 2)Z + (2, 9)Z^2 + (0, 2)Z^3.$$

Teorema 2.4: Con las dos operaciones anteriores $D[Z]$ es un *anillo conmutativo con unidad*.

El elemento idéntico para la multiplicación es

$$\mathbf{1} = (1, 0) + (0, 0)Z + (0, 0)Z^2 + \cdots + (0, 0)Z^j + (0, 0)Z^{j+1} + \ldots$$

El conjunto de los polinomios con la adición y la multiplicación *no forman un dominio de integridad*, debido a la existencia de elementos divisores de cero, es decir, elementos diferentes de $\mathbf{0} = (0, 0) + (0, 0)\ Z + (0, 0)Z^2 + \cdots + (0, 0)Z^j + (0, 0)Z^{j+1} + \ldots$ tales que su producto es **0**. En $D[Z]$ los *divisores de cero* corresponden a polinomios de la forma

$$g(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_k Z^k$$

con b_i en D nilpotente, para todo $i \geq 0$.

2.3. UNIDADES EN D[Z]

Teorema 2.5: Las unidades en $D[Z]$ son de la forma

$$u(Z) = u_0 + u_1 Z + u_2 Z^2 + \cdots + u_n Z^n$$

donde u_0 es un número dual no nilpotente y u_i es un número dual nilpotente para todo $i > 0$.

Demostración:

El polinomio $u(Z)^{-1}$ con u_0 un número dual no nilpotente y u_i un número dual nilpotente para todo $i > 0$, definido por:

$$u(Z)^{-1} = \frac{1}{u_0} - \frac{u_1}{u_0^2} Z - \frac{u_2}{u_0^2} Z^2 - \ldots - \frac{u_n}{u_0^2} Z^n$$

$$u(Z)^{-1} = \frac{1}{u_0^2} (u_0 - u_1 Z - u_2 Z^2 - \cdots - u_n Z^n)$$

está en $D[Z]$ y es el inverso de $u(Z)$, puesto que

$$u(Z)\, u(Z)^{-1} = c_0 + c_1\, Z + c_2\, Z^2 + \cdots + c_r\, Z^r$$

donde

$$c_0 = u_0 \frac{1}{u_0} = 1$$

los c_i con $i > 1$ son 0 pues en cada uno el primer término es el inverso aditivo del último y en los demás se presenta un producto de dos números nilpotentes que siempre es 0:

$$c_1 = u_0\left(-\frac{u_1}{u_0^2}\right) + u_1 \frac{1}{u_0}$$

$$c_2 = u_0\left(-\frac{u_2}{u_0^2}\right) + u_1\left(-\frac{u_1}{u_0^2}\right) + u_2 \frac{1}{u_0}$$

...

$$c_p = u_0\left(-\frac{u_p}{u_0^2}\right) + u_1\left(-\frac{u_{p-1}}{u_0^2}\right) + u_2\left(-\frac{u_{p-2}}{u_0^2}\right) + \cdots + u_p \frac{1}{u_0}$$

Por tanto

$$u(Z)\, u(Z)^{-1} = 1 + 0Z + 0\, Z^2 + \cdots + 0Z^r\,.$$

Ejemplo:

i. En $D[Z]$ el polinomio

$$p(Z) = 5 + (0, 3)Z + (0, 4)\, Z^2 + (0, 2)\, Z^3$$

tiene como inverso

$$p(Z)^{-1} = \frac{1}{5} - \frac{(0, 3)}{5^2} Z - \frac{(0, 4)}{5^2}\, Z^2 - \frac{(0, 2)}{5^2}\, Z^3.$$

ii. En $D[Z]$ el polinomio

$$p(Z) = (1, 2) + (0, 2)\, Z^2 + (0, 1)\, Z^3$$

tiene como inverso

$$p(Z)^{-1} = (1, -2) - (0, 2)\, Z^2 - (0, 1)\, Z^3.$$

Teorema 2.6:* El conjunto de unidades $U(D[Z])$ de $D[Z]$, es un grupo abeliano para la operación de multiplicación en $D[Z]$.

2.4. DIVISIBILIDAD EN D[Z]

Definición 2.8: Dados dos polinomios $p(Z)$ y $q(Z)$ en $D[Z]$, se dice que $p(Z)$ *divide* a $q(Z)$, o que $p(Z)$ es un *divisor* de $q(Z)$, o que $q(Z)$ es un *múltiplo* de $p(Z)$ (representado como $p(Z)|q(Z)$) si existe un polinomio $t(Z)$ en $D[Z]$ tal que $q(Z) = p(Z)\, t(Z)$.

Teorema 2.7:* La relación de divisibilidad es reflexiva y transitiva.

Teorema 2.8:* Dados $p(Z)$, $q(Z)$, $s(Z)$ y $t(Z)$ en $D[Z]$, si $p(Z)|q(Z)$ y $t(Z)|s(Z)$ entonces $p(Z)t(Z)|q(Z)\, s(Z)$.

Teorema 2.9:* Para todo $p(Z)$, $q(Z)$ y $s(Z)$ en $D[Z]$, si $p(Z)|q(Z)$ y $p(Z)|s(Z)$, entonces $p(Z)|(q(Z) + s(Z))$.

Teorema 2.10:* Para todo $p(Z)$, $q(Z)$ y $s(Z)$ en $D[Z]$, si $p(Z)|q(Z)$, entonces $p(Z)|q(Z)\, s(Z)$.

Teorema 2.11:* Las unidades dividen a todo elemento de $D[Z]$.

Demostración:

Si $u(Z)$ es una unidad, cualquier elemento $p(Z)$ de $D[Z]$ se expresa como

$$p(Z) = u(Z)(u(Z)^{-1}\, p(Z)),$$

luego $u(Z)|p(Z)$.

Teorema 2.12:* Los divisores de las unidades son las unidades.

Demostración:
Si $u(Z)$ es una unidad y $p(Z)|u(Z)$, entonces existe un $q(Z)$ en $D[Z]$ tal que $u(Z) = p(Z)\, q(Z)$, luego $\mathbf{1} = p(Z)\, q(Z)\, u(Z)^{-1}$, es decir, $p(Z)$ es una unidad.

2.5. ASOCIADOS EN D[Z]

Definición 2.9: Un elemento $p(Z)$ en $D[Z]$ es un *asociado* de un elemento $s(Z)$ en $D[Z]$ si existe una unidad $u(Z)$ en $D[Z]$ tal que $p(Z) = u(Z)s(Z)$, en otras palabras, $p(Z)$ y $s(Z)$ son asociados si $p(Z)|s(Z)$ y $s(Z)|p(Z)$.

Teorema 2.13:* La relación de asociación es una relación de equivalencia sobre $D[Z]$.

Teorema 2.14: Los polinomios asociados a un polinomio nilpotente $n(Z) = c_0 + c_1Z + c_2 Z^2 + \cdots + c_n Z^n$ en $D[Z]$ son polinomios nilpotentes de la forma $u_0\, n(Z)$ donde u_0 es un elemento en D no nilpotente.

Demostración:
Como toda unidad en $D[Z]$ es de la forma $u(Z) = u_0 + u_1Z + u_2 Z^2 + \cdots + u_k Z^k$ donde u_0 es no nilpotente y u_i es nilpotente para todo número natural $i \neq 0$,

$$u(Z)\, n(Z) = b_0 + b_1\, Z + b_2 Z^2 + \cdots + b_r Z^r$$

donde

$b_0 = c_0u_0$

$b_1 = c_0u_1 + c_1u_0$

$b_2 = c_0u_2 + c_1u_1 + c_2u_0$

$b_3 = c_0u_3 + c_1u_2 + c_2u_1 + c_3u_0$

...

$b_p = c_0u_p + c_1u_{p-1} + c_2u_{p-2} + \cdots + c_pu_0$

y como el producto de dos nilpotentes es igual a 0,

$b_0 = c_0u_0$

$b_1 = c_1u_0$

$b_2 = c_2u_0$

$b_3 = c_3u_0$

...

$b_p = c_pu_0$

luego

$$u(Z)\, n(Z) = u_0\, n(Z).$$

Teorema 2.15: Los polinomios asociados a un polinomio $h(Z) = c_0 + c_1Z + c_2 Z^2 + \cdots + c_n Z^n$ en $D[Z]$ de grado $n > 0$ donde existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente, son polinomios de la forma

$$u_0\, h(Z) + c_i\, Z^i\, (u(Z) - u_0)$$

donde $u(Z) = u_0 + u_1Z + u_2 Z^2 + \cdots + u_k Z^k$ es una unidad.

Demostración:

El producto

$$u(Z)\, h(Z) = b_0 + b_1\, Z + b_2\, Z^2 + \cdots + b_r\, Z^r$$

donde $r = k + i$ tiene como coeficientes a

$b_0 = c_0u_0$

$b_1 = c_0u_1 + c_1u_0$

$b_2 = c_0u_2 + c_1u_1 + c_2u_0$

$b_3 = c_0u_3 + c_1u_2 + c_2u_1 + c_3u_0$

...

$b_i = c_0u_i + c_1u_{i-1} + c_2u_{i-2} + \cdots + c_iu_0$

$b_{i+1} = c_0u_{i+1} + c_1u_i + c_2u_{i-1} + \cdots + c_iu_1 + c_{i+1}u_0$

$b_{i+2} = c_0u_{i+2} + c_1u_{i+1} + c_2u_i + \cdots + c_iu_2 + c_{i+1}u_1 + c_{i+2}u_0$

...

$b_n = c_0u_n + c_1u_{n-1} + c_2u_{n-2} + \cdots + c_iu_{n-i} + \ldots + c_nu_0$

$b_{n+1} = c_0u_{n+1} + c_1u_n + c_2u_{n-1} + \cdots + c_iu_{(n+1)-i} + c_nu_1 + c_{n+1}u_0$

...

$b_r = c_0u_{k+i} + c_1u_{(k+i)-1} + c_2u_{(k+i)-2} + \cdots + c_iu_k + \ldots + c_{(k+i)}u_0$

Como u_0, c_i son no nilpotentes, los c_j con $0 \leq j \leq n$ y $i \neq j$ son nilpotentes, los u_l con $1 \leq l \leq n$ son nilpotentes y el producto de dos nilpotentes es igual a 0, entonces

$b_0 = c_0u_0$

$b_1 = c_1u_0$

$b_2 = c_2u_0$

$b_3 = c_3u_0$

...

$b_i = c_iu_0$

$b_{i+1} = c_iu_1 + c_{i+1}u_0$

$b_{i+2} = c_iu_2 + c_{i+2}u_0$

...

$b_n = c_iu_{n-i} + c_nu_0$

$b_{n+1} = c_iu_{(n+1)-i}$

...

$b_r = c_iu_k$

Luego

$$u(Z)\, h(Z) = u_0\, (c_0 + c_1 Z + c_2 Z^2 + \cdots + c_n Z^n) + c_i Z^i\, (u_1 Z + u_2 Z^2 + \cdots + u_k Z^k)$$

o sea

$$u(Z)\, h(Z) = u_0\, h(Z) + c_i Z^i\, (u(Z) - u_0).$$

2.6. ALGORITMO DE DIVISIÓN EN D[Z]

Teorema 2.16: Dados $p(Z)$ y $q(Z)$ polinomios en $D[Z]$ con $q(Z) \neq 0$ y su coeficiente principal invertible, es decir no nilpotente, existen polinomios $t(Z)$ y $r(Z)$ en $D[Z]$ que son únicos, de manera que se cumple:

$$p(Z) = q(Z)\, t(Z) + r(Z)$$

donde $r(Z) = \mathbf{0}$ ó grado $(r(Z))$ < grado $(q(Z))$.

Demostración:
Se recurre a la inducción sobre el grado de $p(Z)$. Para iniciar se observan varios casos:

Cuando $p(Z) = \mathbf{0}$ se tiene la condición haciendo que $t(Z) = \mathbf{0} = r(Z)$; cuando el grado $(p(Z))$ < grado $(q(Z))$ se llega a la condición tomando $t(Z) = \mathbf{0}$ y $r(Z) = p(Z)$; y cuando el grado $(p(Z))$ = grado $(q(Z)) = 0$ los dos son elementos del anillo D, la proposición se demuestra escogiendo a $t(Z) = p(Z)q(Z)^{-1}$ y a $r(Z) = \mathbf{0}$.

Falta demostrar el caso donde el grado $(p(Z))$ > grado $(q(Z))$, entonces se inicia la inducción sobre el grado de $p(Z)$, suponiendo que el teorema se cumple para todo polinomio de grado menor que el de $p(Z)$, donde el grado $(p(Z))$ > grado $(q(Z)) > 1$, luego

$$p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n, \quad a_n \neq 0$$
$$q(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_m Z^m, \quad b_m \neq 0$$

Si se divide el termino n-ésimo de $p(Z)$ entre el término m-ésimo de $q(Z)$ se obtiene $(a_n b_m^{-1})Z^{n-m}$.

Al multiplicar $(a_n b_m^{-1})Z^{n-m}$ por $q(Z)$ y el resultado restárselo a $p(Z)$, obtenemos un polimonio $p_1(Z)$ de $D[Z]$, que se expresa como

$$p_1(Z)= p(Z) - (a_n b_m^{-1})Z^{n-m}\, q(Z)$$

y como el coeficiente de Z^n en $p_1(Z)$ es $a_n - (a_n b_m^{-1})b_m = 0$, entonces el

$$\text{grado } (p_1(Z)) < \text{grado } (p(Z))$$

y por la hipótesis de inducción, el teorema se cumple para el polinomio $p_1(Z)$, luego existen $t_1(Z)$, $r(Z)$ en $D[Z]$ tales que

$$p_1(Z) = t_1(Z)\, q(Z) + r(Z)$$

donde $r(Z) = \mathbf{0}$ ó grado $(r(Z)) <$ grado $(q(Z))$. Entonces se obtiene que

$$\begin{aligned} p(Z) &= p_1(Z) + (a_n b_m^{-1})Z^{n-m}\, q(Z) \\ p(Z) &= (t_1(Z)\, q(Z) + r(Z)) + (a_n b_m^{-1})Z^{n-m}\, q(Z) \\ p(Z) &= (t_1(Z) + (a_n b_m^{-1})Z^{n-m})\, q(Z) + r(Z) \end{aligned}$$

Por tanto queda demostrado que el teorema se cumple para cualquier polinomio $p(Z)$.

Para mostrar la unicidad de los polinomios $t(Z)$ y $r(Z)$, se supone que existen otros polinomios $t_0(Z)$ y $r_0(Z)$ tales que

$$p(Z) = q(Z)\, t(Z) + r(Z) = q(Z)\, t_0(Z) + r_0(Z)$$

donde $r(Z) = \mathbf{0} = r_0(Z)$ ó grado $(r(Z))$ < grado $(q(Z))$ y grado $(r_0(Z))$ < grado $(q(Z))$.

Entonces:

$$r(Z) - r_0(Z) = (t_0(Z) - t(Z))\, q(Z)$$

Si se supone que $t_0(Z) - t(Z) \neq \mathbf{0}$ y como el coeficiente principal de $q(Z)$ es invertible, es decir no nilpotente, entonces

$$\text{grado } ((t_0(Z) - t(Z))q(Z)) = \text{grado } (t_0(Z) - t(Z)) + \text{grado } (q(Z)),$$

y como

$$\text{grado } (t_0(Z) - t(Z)) + \text{grado } (q(Z)) \geq \text{grado } (q(Z))$$

entonces

$$\text{grado } ((t_0(Z) - t(Z))q(Z)) \geq \text{grado } (q(Z))$$

pero como

$$\text{grado } (r(Z) - r_0(Z)) < \text{grado } (q(Z)),$$

se llega a una contradicción. Por lo tanto $t_0(Z) = t(Z)$ y en consecuencia $r(Z) = r_0(Z)$.

2.7. HOMOMORFISMO DE EVALUACIÓN

Teorema 2.17:* La función $e_z : D[Z] \to D$ que a todo polinomio $p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$ con $a_n \neq 0$, le asigna $a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$ con z en D, es un homomorfismo de anillos, puesto que D es conmutativo. Este homomorfismo es llamado *homomorfismo de evaluación*.

Es importante recalcar que D sea conmutativo, pues si no lo fuera, entonces:

$$\begin{aligned} e_z[(a_0 + a_1Z)(b_0 + b_1Z)] &= e_z[a_0b_0 + (a_0b_1 + a_1b_0)Z + (a_1b_1)Z^2] \\ &= a_0b_0 + (a_0b_1 + a_1b_0)z + (a_1b_1)z^2 \end{aligned}$$

y

$$e_z(a_0 + a_1Z)\, e_z(b_0 + b_1Z) = (a_0 + a_1z)(\, b_0 + b_1z)$$
$$= a_0b_0 + a_0b_1z + a_1zb_0 + a_1zb_1z$$

no serían necesariamente iguales.

2.8. TEOREMA DEL RESIDUO

Teorema del residuo 2.18:* Dado $p(Z)$ en $D[Z]$ y a en D, existe un único polinomio $q(Z)$ en $D[Z]$ tal que

$$p(Z) = q(Z)(Z - a) + p(a).$$

Demostración:
Aplicando el algoritmo de división a los polinomios $p(Z)$ y $(Z - a)$ se tiene que

$$p(Z) = q(Z)(Z - a) + r(Z)$$

donde el grado de $r(Z)$ es menor que 1, es decir, $r(Z)$ es una constante. Aplicando el homomorfismo de evaluación en a:

$$e_a\,(p(Z)) = e_a(q(Z)(Z - a) + r)$$
$$p(a) = q(a)(a - a) + r$$

se tiene que $r = p(a)$.

2.9. TEOREMA DEL FACTOR

Definición 2.10: Si $p(Z)$ es un polinomio de $D[Z]$ entonces a en D es una raíz de $p(Z)$ si $e_a\,(p(Z)) = 0$.

Teorema del factor 2.19:* Si $p(Z)$ es un polinomio de $D[Z]$ entonces a en D es una raíz de $p(Z)$ si y sólo si $Z - a | p(Z)$.

Demostración:
Si a en D es una raíz de $p(Z)$, entonces $e_a\,(p(Z)) = 0$ y por el teorema del residuo se tiene que $p(Z) = q(Z)(Z - a)$, luego $Z - a | p(Z)$.

Si $Z - a | p(Z)$ entonces $p(Z) = q(Z)(Z - a)$ y aplicando el homomorfismo de evaluación en a se tiene que

$$e_a\,(p(Z)) = e_a(q(Z)(Z - a))$$
$$p(a) = q(a)(a - a) = 0,$$

luego a en D es una raíz de $p(Z)$.

En el anillo de polinomios $K[x]$ con K un campo se cumple el teorema que dice: *Si* $p(x)$ *es un polinomio distinto de* **0** *en* $K[x]$ *de grado* n, *entonces* $p(x)$ *tiene a lo más* n *raíces en* K.

En $D[Z]$ no se cumple este teorema pues se tiene los polinomios de grado n de la forma

$$p(Z) = a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$$

con a_1 nilpotente, tienen *infinitas raíces*: los nilpotentes en D, es decir los números de la forma $(0, b)$ con b en los números reales.

2.10. IDEALES EN D[Z]

Teorema 2.20: En $D[Z]$ el conjunto $N[Z]$ de todos los polinomios nilpotentes es un ideal principal.

Demostración:
Los polinomios nilpotentes son los que tienen todos los coeficientes nilpotentes y si se multiplica un elemento nilpotente $c \neq 0$ en D por un polinomio cualquiera en $D[Z]$ todos los coeficientes del producto son nilpotentes, esto es, $\langle c \rangle = \{c\, q(Z) : q(Z) \in D[Z]\}$.

Además, todo polinomio nilpotente se puede escribir como el producto de un polinomio $p(Z)$ en $D[Z]$ por un elemento nilpotente $(0, d)$ distinto de 0 en D, pues cada uno de sus coeficientes es de la forma $(0, m)$ y la ecuación

$$(0, m) = (0, d)\,(x, y)$$

siempre tiene solución en D. Por lo tanto el conjunto de todos los polinomios nilpotentes es un ideal principal generado por cualquier elemento nilpotente en D.

Teorema 2.21: En $D[Z]$ el conjunto $Z\,p(Z)$ de todos los polinomios sin coeficiente constante es un ideal principal.

Demostración:
Los polinomios sin coeficiente constante son de la forma $Z\,p(Z)$ para algún $p(Z)$ en $D[Z]$ y $\langle Z \rangle = \{Z\, q(Z) : q(Z) \in D[Z]\}$, luego el conjunto de todos los polinomios sin coeficiente constante es un ideal principal generado por el polinomio Z.

*Teorema 2.22**: Si I, J son ideales en $D[Z]$ entonces $I \cap J$ es un ideal en $D[Z]$.

*Teorema 2.23**: Si I, J son ideales en $D[Z]$ entonces $I + J = \{i + j: i \in I, \wedge, j \in J\}$ es un ideal en $D[Z]$.

Teorema 2.24: El subconjunto $Z\,N[Z] = Z\,p(Z) \cap N[Z]$ de $D[Z]$ es un ideal principal.

Demostración:

Los polinomios nilpotentes sin coeficiente constante son de la forma $c_1 Z\ p(Z)$ con c_1 nilpotente en D y $\langle cZ\rangle = \{cZ\ q(Z) : c^2 = 0, \wedge, q(Z) \in D[Z]\}$, luego el conjunto de todos los polinomios nilpotentes sin coeficiente constante es un ideal principal generado por el polinomio cZ con c nilpotente.

Teorema 2.25: El subconjunto $N[Z] + Z\,p(Z)$ de $D[Z]$ es un ideal principal.

Demostración:

Los polinomios con coeficiente constante nilpotente son de la forma $a_0 + a_1 Z + \cdots + a_n Z^n$ con a_0 nilpotente y si se multiplica el polinomio $c_0 + c_1 Z$ con c_0 nilpotente distinto de 0 y c_1 no nilpotente, por un polinomio cualquiera en $D[Z]$, el coeficiente constante del producto será nilpotente, esto es,

$$\langle c_0 + c_1 Z\rangle = \{(c_0 + c_1 Z)\ q(Z) : (c_0)^2 = 0, \wedge,\ c_0 \neq 0,\ \wedge, (c_1)^2 \neq 0, \wedge, q(Z) \in D[Z]\}.$$

Además, todo polinomio $q(Z) = d_0 + d_1 Z + \cdots + d_n Z^n$ con coeficiente constante nilpotente se puede escribir como el producto de un polinomio $p(Z) = b_0 + b_1 Z + \cdots + b_k Z^k$ en $D[Z]$ por el polinomio $c_0 + c_1 Z$ con c_0 nilpotente distinto de 0 y c_1 no nilpotente, pues cada uno de sus coeficientes debe ser de la forma

$$d_i = c_0\, b_i\ +\ c_1\, b_{i-1}$$

y como $c_0 = (0,\ t)$ con $t \neq 0$, $c_1 = (x,\ y)$ con $x \neq 0$, se debe encontrar $b_i = (a,\ b)$ y $b_{i-1} = (c,\ d)$ y esto siempre es posible puesto que la ecuación

$$d_i = (w, z) = (xc,\ at + xd + yc)$$

tiene siempre soluciones en D.

Teorema 2.26: En $D[Z]$ el conjunto $Z^k\, p(Z)$ de todos los polinomios

$$q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$$

cuyos coeficientes $a_i = 0$ con i, k números naturales tales que $0 \leq i < k$ es un ideal principal.

Demostración:
Los polinomios $q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ cuyos coeficientes $a_i = 0$ con i, k números naturales tales que $0 \leq i < k$ son de la forma $Z^k\, p(Z)$ para algún $p(Z)$ en $D[Z]$ y $\langle Z^k \rangle = \{Z^k\, t(Z) : t(Z) \in D[Z]\}$, luego el conjunto $Z^k\, p(Z)$ es un ideal principal generado por el polinomio Z^k.

Corolario 2.1: En $D[Z]$ el conjunto $Z^2\, p(Z)$ de todos los polinomios

$$q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$$

cuyos coeficientes a_0, a_1 son iguales a 0, es un ideal principal.

Demostración:
Los polinomios $q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ cuyos coeficientes $a_0 = 0 = a_1$ son de la forma $Z^2\, p(Z)$ para algún $p(Z)$ en $D[Z]$ y $\langle Z^2 \rangle = \{Z^2\, t(Z) : t(Z) \in D[Z]\}$, luego el conjunto $Z^2\, p(Z)$ es un ideal principal generado por el polinomio Z^2.

Teorema 2.27: El subconjunto $Z^k\, N[Z] = Z^k\, p(Z) \cap N[Z]$ de $D[Z]$ es un ideal principal.

Demostración:
Los polinomios nilpotentes $n(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ cuyos coeficientes $a_i = 0$ con i, k números naturales tales que $0 \leq i < k$ son de la forma $c_1 Z^k\, p(Z)$ con c_1 nilpotente en D y

$\langle cZ^k \rangle = \{cZ^k\, q(Z) : k > 0, \wedge, c^2 = 0, \wedge, q(Z) \in D[Z]\}$, luego el conjunto $Z^k\, N[Z]$ es un ideal principal generado por el polinomio cZ^k con c nilpotente.

Teorema 2.28: El subconjunto $N[Z] + Z^k\, p(Z)$ de $D[Z]$ es un ideal principal.

Demostración:
Si se multiplica el polinomio $c_0 + c_1\, Z + \cdots + c_k\, Z^k$ con c_i nilpotente distinto de 0, $0 \le i \le k - 1$ y c_k no nilpotente, por un polinomio cualquiera $p(Z)$ en $D[Z]$, los coeficientes d_j con $0 \le j \le k - 1$ del producto

$$(c_0 + c_1 Z + \cdots + c_k Z^k)(p(Z)) = d_0 + d_1 Z + \cdots + d_m Z^m$$

son todos nilpotente, esto es,

$\langle c_0 + c_1 Z + \cdots + c_{k+1} Z^k \rangle$
$=\{(c_0 + c_1\, Z + \cdots + c_k\, Z^k)\, q(Z) : 0 \le i \le k - 1, \wedge, c_i \ne 0, \wedge, (c_i)^2 = 0, \wedge, (c_k)^2 \ne 0, \wedge, q(Z) \in D[Z]\}$.

De otro lado, todo polinomio $q(Z) = d_0 + d_1\, Z + \cdots + d_n\, Z^n$ con coeficientes d_j nilpotente, para $0 \le j \le k - 1$, se puede escribir como el producto de un polinomio $p(Z) = b_0 + b_1\, Z + \cdots + b_m\, Z^m$ en $D[Z]$ por el polinomio $c_0 + c_1\, Z + \cdots + c_k\, Z^k$ con c_i nilpotente distinto de 0, $0 \le i \le k - 1$ y c_k no nilpotente, pues cada uno de sus coeficientes debe ser de la forma

$$d_i = c_0\, b_i + c_1\, b_{i-1} + c_2\, b_{i-2} + \ldots + c_{k-1}\, b_{i-(k-1)} + c_k\, b_{i-k}$$

y como $c_0 = (0, t_0)$, $c_1 = (0, t_1)$, $c_2 = (0, t_2)$, …, $c_{k-1} = (0, t_{k-1})$, con $t_0, t_1, t_2, \ldots, t_{k-1}$, distintos de 0, $c_k = (x, y)$, con $x \ne 0$, se debe encontrar $b_i = (a_i, b_i)$, $b_{i-1} = (a_{i-1}, b_{i-1})$,

$b_{i-2} = (a_{i-2}, b_{i-2})$, …, $b_{i-(k-1)} = (a_{i-(k-1)}, b_{i-(k-1)})$, $b_{i-k} = (a_{i-k}, b_{i-k})$, y esto siempre es posible puesto que la ecuación

$$d_i = (w, z) = (x\, a_{i-k}, a_i\, t_0 + a_{i-1}\, t_1 + \ldots + a_{i-(k-1)}\, t_{k-1} + x\, b_{i-k} + y\, a_{i-k})$$

tiene siempre soluciones en D.

Teorema 2.29: Para todo número natural $k > 0$, se cumple que

$$\langle Z^k \rangle \subseteq \langle Z^{k-1} \rangle \subseteq \langle Z^{k-2} \rangle \subseteq \langle Z^{k-3} \rangle \subseteq \ldots \subseteq \langle Z^2 \rangle \subseteq \langle Z \rangle.$$

Demostración:
Por inducción sobre k, el caso para $k = 1$ es evidente.

Se supone que la afirmación es cierta para todo número natural $i < k$, entonces es cierta en particular para $i = k - 1$.

Dado $p(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ en $\langle Z^k \rangle$ por el *teorema 2.26*

$$\langle Z^k \rangle = \{Z^k\, t(Z) : t(Z) \in D[Z]\},$$

luego $a_j = 0$ con $0 \leq j \leq k - 1$ y como

$$\langle Z^{k-1} \rangle = \{Z^{k-1} t(Z) : t(Z) \in D[Z]\}$$

si $s(Z) = b_0 + b_1 Z + \cdots + b_m Z^m$ está en $\langle Z^{k-1} \rangle$, entonces $b_l = 0$ con $0 \leq l \leq k - 2$, por tanto $p(Z)$ está en $\langle Z^{k-1} \rangle$ de donde $\langle Z^k \rangle \subseteq \langle Z^{k-1} \rangle$, y por la hipótesis de inducción

$$\langle Z^k \rangle \subseteq \langle Z^{k-1} \rangle \subseteq \langle Z^{k-2} \rangle \subseteq \langle Z^{k-3} \rangle \subseteq \ldots \subseteq \langle Z^2 \rangle \subseteq \langle Z \rangle.$$

Teorema 2.30: $D[Z]/\langle Z\rangle$ es isomorfo con D.

Demostración:
En el anillo

$$D[Z]/\langle Z\rangle = \{q(Z) + \langle Z\rangle : q(Z) \in D[Z]\}$$

las clases de equivalencia son los polinomios cuyo coeficiente constante es igual. Entonces la función

$$\lambda: D[Z]/\langle Z\rangle \rightarrow D$$
$$q(Z) + \langle Z\rangle \mapsto a_0$$

con $q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$, es un homomorfismo puesto que dados

$$t(Z) = a_0 + a_1 Z + \cdots + a_n Z^n \quad \text{y} \quad s(Z) = b_0 + b_1 Z + \cdots + b_k Z^k$$

$$\begin{aligned}\lambda\,[(t(Z) + \langle Z\rangle) + (s(Z) + \langle Z\rangle)] &= \lambda\,[(t(Z) + s(Z)) + \langle Z\rangle] \\ &= a_0 + b_0 \\ &= \lambda\,[(t(Z) + \langle Z\rangle)] + \lambda\,[(s(Z) + \langle Z\rangle)]\end{aligned}$$

$$\begin{aligned}\lambda\,[(t(Z) + \langle Z\rangle)\,(s(Z) + \langle Z\rangle)] &= \lambda\,[(t(Z)\,s(Z)) + \langle Z\rangle] \\ &= a_0\,b_0 \\ &= \lambda\,[(t(Z) + \langle Z\rangle)]\;\lambda\,[(s(Z) + \langle Z\rangle)]\end{aligned}$$

Además λ es inyectiva ya que $N_\lambda = \{\langle Z\rangle\}$ y λ es sobreyectiva pues dado a en D, existe la clase de polinomios en $D[Z]/\langle Z\rangle$ cuyo coeficiente constante es a.

Teorema 2.31: En $D[Z]$ el ideal principal $Z\,p(Z)$ no es un ideal maximal.

Demostración:
Por el *teorema 1.73* y el *teorema 2.30* se concluye que $Z\,p(Z)$ no es un ideal maximal.

Teorema 2.32: $Z\,p(Z)$ no es un ideal primo.

2.11. POLINOMIOS IRREDUCIBLES EN D[Z]

Las afirmaciones que se muestran a continuación sobre polinomios irreducibles en $D[Z]$ están a nivel de conjetura, fruto de los casos estudiados, porque al realizar intentos de demostración, éstos incluyen dos casos: uno en el que el producto de los coeficientes $a_i b_j$ de los polinomios considerados como factores sean todos iguales a 0 y el otro cuando uno de los productos $a_i b_j$ es el inverso aditivo de la suma de los demás. Este último caso no ha sido considerado en los intentos de demostración pero se sospecha que no se puede dar cuando se fijan los grados de los polinomios producto.

Afirmación 2.1: Un polinomio $h(Z) = c_0$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 es nilpotente.

Prueba parcial:
Si $h(Z) = c_0$ y $h(Z) = p(Z)q(Z)$ con

$$p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_r Z^r\,,\ \ a_r \neq 0$$
$$q(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_s Z^s,\quad b_s \neq 0$$

de manera que $0 \leq r + s$, entonces se deben buscar las condiciones sobre los coeficientes de $p(Z)$ y $q(Z)$ para que al realizar el producto se obtenga $h(Z)$.

Para que $c_0 = a_0 b_0$ sea nilpotente, es necesario que uno de los factores sea nilpotente y el otro no nilpotente.

Si a_0 es no nilpotente y b_0 es nilpotente, entonces dados

$c_1 = a_0b_1 + a_1b_0$

$c_2 = a_0b_2 + a_1b_1 + a_2b_0$

$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$

...

$c_p = a_0b_p + a_1b_{p-1} + a_2b_{p-2} + \cdots + a_pb_0$

los c_i con $1 \leq i \leq n$ deben ser iguales a 0, entonces si cada producto es cero, y como se tiene que a_0 es no nilpotente, observando la columna donde aparece a_0, resulta que los b_m con $1 \leq m \leq s$ deben ser iguales a 0. También se tiene que b_0 es nilpotente y observando la columna donde éste aparece, se obtiene que los a_j con $1 \leq j \leq r$ deben ser nilpotentes o iguales a 0. Con esas dos nuevas condiciones los otros productos que se presentan son iguales a 0.

Entonces $p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r$, debe cumplir que a_0 sea no nilpotente y los a_j con $1 \leq j \leq r$ sean nilpotentes o iguales a 0, es decir, son unidades. Y $q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s$, debe cumplir que b_0 sea nilpotente y los b_m con $1 \leq m \leq s$ sean iguales a 0, es decir, es una no unidad.

Por tanto un polinomio $h(Z) = c_0$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 es nilpotente y se cumplen las condiciones dadas.

Afirmación 2.2: Un polinomio $h(Z) = c_0 + c_1Z$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 y c_1 son no nilpotentes.

Prueba parcial:

Si $h(Z) = c_0 + c_1Z$ y $h(Z) = p(Z)q(Z)$ con

$$p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r, \quad a_r \neq 0$$

$$q(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_s Z^s, \quad b_s \neq 0$$

de manera que $1 \leq r + s$, entonces se deben buscar las condiciones sobre los coeficientes de $p(Z)$ y $q(Z)$ para que al realizar el producto se obtenga $h(Z)$.

Para que $c_0 = a_0 b_0$ sea no nilpotente, es necesario que los dos factores sean no nilpotentes.

Si a_0 y b_0 son no nilpotentes, entonces para que $c_1 = a_0 b_1 + a_1 b_0$ sea no nilpotente se dan los siguientes casos:

a_1	b_1
No nilpotente	No nilpotente
No nilpotente	Nilpotente
No nilpotente	0
Nilpotente	No nilpotente
0	No nilpotente

Y como

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$

...

$c_p = a_0 b_p + a_1 b_{p-1} + a_2 b_{p-2} + \cdots + a_p b_0$

los c_i con $2 \leq i \leq n$ deben ser iguales a 0, entonces si cada producto es cero, $a_1 b_1 = 0$, implica que de las opciones mencionadas sólo son posibles aquellas donde a_1 es no nilpotente y b_1 es 0, o cuando a_1 es 0 y b_1 es no nilpotente.

Como se tiene que a_0 es no nilpotente y $a_0 b_m = 0$ con $2 \leq m \leq s$ entonces los b_m deben ser iguales a 0. Análogamente como b_0 es no nilpotente, los a_j con $2 \leq j \leq r$ deben ser iguales a 0. Con esas condiciones los otros productos que se presentan son iguales a 0.

Entonces si $p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_r Z^r$, cumple que a_0 es no nilpotente, a_1 es no nilpotente y los a_j con $2 \leq j \leq r$ son iguales a 0, es decir, son no unidades; $q(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_s Z^s$, debe cumplir que b_0 sea no nilpotente, b_1 sea igual a 0 y los b_m con $2 \leq m \leq s$ sean iguales a 0, es decir, es una unidad.

Y si $p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_r Z^r$, cumple que a_0 es no nilpotente, a_1 es igual a 0 y los a_j con $2 \leq j \leq r$ son iguales a 0, es decir, son unidades; $q(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_s Z^s$, debe cumplir que b_0 sea no nilpotente, b_1 sea no nilpotente y los b_m con $2 \leq m \leq s$ sean iguales a 0, es decir, es una no unidad.

Por tanto un polinomio $h(Z) = c_0 + c_1 Z$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 y c_1 son no nilpotentes y se cumplen las condiciones dadas.

Afirmación 2.3: Un polinomio $h(Z) = c_0 + c_1 Z + c_2 Z^2 + \cdots + c_n Z^n$ en $D[Z]$ de grado $n > 0$ es irreducible en $D[Z]$, si existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente.

Demostración:
Se recurre a la inducción sobre el grado de $h(Z)$. Para iniciar se observa que cuando $n = 1$ se tienen tres casos:

i. Sea $h(Z) = c_0 + c_1 Z$ donde c_0 y c_1 son nilpotentes. En este caso, se puede expresar un polinomio $h(Z)$ con las condiciones dadas, por ejemplo, $h(Z) = (0, 2) + (0, 4)Z$ como un producto de dos polinomios $p(Z)$ y $q(Z)$ que no son unidades:

Dado $p(Z) = (0, 2)$ y $q(Z) = (1, 2) + (2, 1)Z$ el producto $p(Z)q(Z)$ es $h(Z)$.
Dado $p(Z) = (0, 2)$ y $q(Z) = (1, 2) + (2, 1)Z + (0, 3)Z^2$ el producto $p(Z)q(Z)$ es $h(Z)$.

Luego es reducible.

ii. Sea $h(Z) = c_0 + c_1Z$ donde c_0 y c_1 son no nilpotentes. En este caso de acuerdo a la *afirmación 2.2* se tiene que los polinomios que tienen esa forma son irreducibles si cumplen las condiciones dadas.

iii. Sea $h(Z) = c_0 + c_1Z$ donde c_0 es nilpotente y c_1 es no nilpotente.

Si $h(Z) = c_0 + c_1Z$ y $h(Z) = p(Z)q(Z)$ con

$$p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r, \quad a_r \neq 0$$
$$q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s, \quad b_s \neq 0$$

de manera que $1 \leq r + s$, entonces se deben buscar las condiciones sobre los coeficientes de $p(Z)$ y $q(Z)$ para que al realizar el producto se obtenga $h(Z)$.

Para que $c_0 = a_0b_0$ sea nilpotente, es necesario que uno de los factores sea nilpotente y el otro no nilpotente.

Si a_0 es nilpotente y b_0 es no nilpotente, entonces para que $c_1 = a_0b_1 + a_1b_0$ sea no nilpotente se dan los siguientes casos:

a_1	b_1
No nilpotente	No nilpotente
No nilpotente	Nilpotente
No nilpotente	0

Y como

$c_2 = a_0b_2 + a_1b_1 + a_2b_0$

$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$

...

$c_p = a_0b_p + a_1b_{p-1} + a_2b_{p-2} + \cdots + a_pb_0$

los c_i con $2 \leq i \leq n$ deben ser iguales a 0, entonces si cada producto es cero, $a_1b_1 = 0$, implica que de las opciones mencionadas sólo es posible aquella donde a_1 es no nilpotente y b_1 es 0.

Como se tiene que a_0 es nilpotente y $a_0b_m = 0$ con $2 \leq m \leq s$ entonces los b_m deben ser nilpotentes o iguales a 0. También como b_0 es no nilpotente, los a_j con $2 \leq j \leq r$ deben ser iguales a 0. Pero con esas condiciones no se puede asegurar que los otros productos que se presentan son iguales a 0, pues como a_1 es no nilpotente, para que $a_1b_m = 0$ con $2 \leq m \leq s$, los b_m sólo deben ser iguales a 0.

Entonces $p(Z) = a_0 + a_1Z + a_2 Z^2 + \cdots + a_r Z^r$, debe cumplir que a_0 sea nilpotente, a_1 sea no nilpotente y los a_j con $2 \leq j \leq r$ sean iguales a 0, es decir, son no unidades. Y $q(Z) = b_0 + b_1Z + b_2 Z^2 + \cdots + b_s Z^s$, debe cumplir que b_0 sea no nilpotente y los b_m con $1 \leq m \leq s$ sean iguales a 0, es decir, es una unidad.

Por tanto un polinomio $h(Z) = c_0 + c_1Z$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 es nilpotente y c_1 es no nilpotente y se cumplen las condiciones dadas.

Si para algún número natural $n > 0$, un polinomio $h(Z) = c_0 + c_1Z + c_2 Z^2 + \cdots + c_n Z^n$ en $D[Z]$, en el cual existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente, se tiene que $h(Z)$ es irreducible.

Se debe probar que todo polinomio de grado $n + 1$ que cumpla las condiciones es irreducible.

Todo polinomio $p(Z)$ de grado $n + 1$ en $D[Z]$ que satisfaga las condiciones de la *afirmación 2.3* es de la forma

$$p(Z) = x_0 + Zh(Z) \text{ con } x_0 \text{ nilpotente}$$

o

$$p(Z) = h(Z) + c_{n+1} Z^{n+1} \text{ con } c_{n+1} \text{ nilpotente,}$$

pues si $h(Z) = c_0 + c_1 Z + c_2 Z^2 + \cdots + c_n Z^n$ donde existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente, para obtener un polinomio de grado $n + 1$ que cumpla también las condiciones se dan los siguientes casos:

i. Multiplicar $h(Z)$ por el polinomio Z y al polinomio resultante sumarle un elemento x_0 nilpotente en D.

ii. Al polinomio $h(Z)$ sumarle el polinomio $c_{n+1} Z^{n+1}$ con c_{n+1} nilpotente en D.

iii. Se multiplica el polinomio Z por el polinomio $c_j Z^j + c_{j+1} Z^{j+1} + c_{j+2} Z^{j+2} + \cdots + c_n Z^n$ para algún $j \leq n$ obteniéndose como resultado

$$c_j Z^{j+1} + c_{j+1} Z^{j+2} + c_{j+2} Z^{j+3} + \cdots + c_n Z^{n+1}$$

luego a este polinomio se le suma $c_0 + c_1 Z + c_2 Z^2 + \cdots + c_{j-1} Z^{j-1}$ pero hace falta el j-ésimo término por tanto el polinomio de grado $n + 1$ queda de la forma:

$$c_0 + c_1 Z + c_2 Z^2 + \cdots + c_{j-1} Z^{j-1} + q Z^j + c_j Z^{j+1} + c_{j+1} Z^{j+2} + c_{j+2} Z^{j+3} + \cdots + c_n Z^{n+1}$$

para algún q no nilpotente.

El caso *iii*. se reduce al *i*. si $j = 0$ y se reduce al *ii*. si $1 \leq j \leq n$, por tanto dado un polinomio $h(Z)$ que cumpla las condiciones sólo existen dos formas diferentes de conseguir un polinomio de grado $n + 1$ que también cumpla las condiciones.

Si $p(Z) = x_0 + Zh(Z)$ con x_0 nilpotente, se debe probar que es irreducible. Si $p(Z)$ no es irreducible existen $q(Z) = a_0 + a_1Z + a_2 Z^2 + \cdots + a_u Z^u$ y $r(Z) = b_0 + b_1Z + b_2 Z^2 + \cdots + b_v Z^v$ tales que $p(Z) = q(Z)\, r(Z)$ donde $q(Z)$ y $r(Z)$ no son unidades; entonces

$$q(Z)\, r(Z) = x_0 + Zh(Z)$$

y para que $x_0 = a_0b_0$ sea nilpotente, es necesario que uno de los factores sea nilpotente y el otro no nilpotente o los dos sean nilpotentes.

Si a_0 es nilpotente, b_0 es no nilpotente y existe al menos un b_g para algún número natural $1 \leq g \leq n$ que sea no nilpotente, pues $r(Z)$ no es unidad, para cumplir las condiciones es necesario que sólo uno de los coeficientes del producto sea no nilpotente, entonces puede darse que:

Si b_{i-j} con $1 \leq i - j \leq n$ es no nilpotente y se elige que $c_{i-1}Z^{\,i}$ sea el coeficiente no nilpotente en el producto,

$c_0 = a_0b_1 + a_1b_0$

$c_1 = a_0b_2 + a_1b_1 + a_2b_0$

$c_2 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$

...

$c_{j-1} = a_0b_j + a_1b_{j-1} + a_2b_{j-2} + \cdots + a_jb_0$

$c_j = a_0b_{j+1} + a_1b_j + a_2b_{j-1} + \cdots + a_jb_1 + a_{j+1}b_0$

...

$c_{i-1} = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_jb_{i-j} + a_{j+1}\, b_{i-(j+1)} + \ldots + a_ib_0$

$c_i = a_0b_{i+1} + a_1b_i + a_2b_{i-1} + \cdots + a_jb_{\,i+1-j} + \ldots + a_ib_1 + a_{i+1}b_0$

…

$c_{t-1} = a_0 b_t + a_1 b_{t-1} + a_2 b_{t-2} + \cdots + a_j b_{t-j} + \ldots + a_t b_0$

entonces es necesario que por lo menos uno de los sumandos sea no nilpotente, por ejemplo $a_j b_{i-j}$, por tanto a_j debe también ser no nilpotente. Pero si a_j es no nilpotente el producto $a_j b_0$ sería no nilpotente pues b_0 es no nilpotente y el coeficiente c_{j-1} sería también no nilpotente, lo que contradice la hipótesis.

Otra opción es elegir b_{i-j} con $1 \leq i - j \leq n$ no nilpotente y c_{t-1} como el coeficiente no nilpotente en el producto, entonces es necesario que por lo menos uno de los sumandos sea no nilpotente, por ejemplo $a_j b_{t-j}$, por tanto a_j y b_{t-j} deben ser no nilpotentes. Pero si a_j es no nilpotente los productos $a_j b_0$, $a_j b_{i-j}$ serían no nilpotentes y los coeficientes c_{j-1}, c_{i-1} también lo serían, lo que contradice la hipótesis.

Ahora, si a_0 y b_0 son nilpotentes, para cumplir las condiciones es necesario que sólo uno de los coeficientes del producto sea no nilpotente, por ejemplo c_{i-1}:

$c_0 = a_0 b_1 + a_1 b_0$

$c_1 = a_0 b_2 + a_1 b_1 + a_2 b_0$

$c_2 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$

...

$c_{i-2} = a_0 b_{i-1} + a_1 b_{i-2} + a_2 b_{i-3} + \cdots + a_j b_{i-1-j} + \ldots + a_{i-2} b_1 + a_{i-1} b_0$

$c_{i-1} = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_j b_{i-j} + a_{j+1} b_{i-(j+1)} + \ldots + a_i b_0$

$c_i = a_0 b_{i+1} + a_1 b_i + a_2 b_{i-1} + \cdots + a_j b_{i+1-j} + a_{j+1} b_{i-j} + \ldots + a_i b_1 + a_{i+1} b_0$

entonces es necesario que por lo menos uno de los sumandos sea no nilpotente, por ejemplo $a_j b_{i-j}$, por tanto a_j y b_{i-j} deben ser no nilpotentes. Pero puede haber otro sumando, por ejemplo $a_{j+1} b_{i-(j+1)}$, donde a_{j+1} sea nilpotente y $b_{i-(j+1)}$ sea no nilpotente; o a_{j+1} sea no nilpotente y $b_{i-(j+1)}$ sea no nilpotente; o a_{j+1} sea no nilpotente y $b_{i-(j+1)}$ sea nilpotente,

que no afecta que c_{i-1} sea no nilpotente pero que si causa que otros coeficientes lo sean, presentándose una contradicción:

Si a_{j+1} es nilpotente y $b_{i-(j+1)}$ es no nilpotente, el producto $a_j b_{i-1-j}$ sería no nilpotente y el coeficiente c_{i-2} sería no nilpotente.

Si a_{j+1} es no nilpotente y $b_{i-(j+1)}$ es no nilpotente, el producto $a_{j+1}\, b_{i-j}$ sería no nilpotente y el coeficiente c_i sería no nilpotente.

Si a_{j+1} es no nilpotente y $b_{i-(j+1)}$ es nilpotente, el producto $a_{j+1}\, b_{i-j}$ sería no nilpotente y el coeficiente c_i sería no nilpotente.

Por tanto, el polinomio $p(Z) = x_0 + Zh(Z)$ con x_0 nilpotente, es irreducible.

De manera análoga se obtiene que el polinomio $p(Z) = h(Z) + c_{n+1} Z^{n+1}$ con c_{n+1} nilpotente, es irreducible.

CONCLUSIONES

El anillo de los números duales es un ejemplo interesante que permite ilustrar situaciones algebraicas que no son frecuentes en la teoría de anillos y campos que se estudia en la Licenciatura en Matemáticas de la Universidad Pedagógica Nacional, un ejemplo de ello es que a pesar de que D no es un dominio de integridad la propiedad cancelativa es válida para todos los elementos no nilpotentes; la función logaritmo, que en el caso de los números complejos tiene varias ramas, lo que dificulta su estudio y aplicación, en los números duales es una función biyectiva; en el anillo de polinomios con coeficientes en los números duales existen polinomios no constantes que tienen inverso multiplicativo, polinomios con infinitas raíces diferentes y el grado del producto de dos polinomios no en todos los casos es igual a la suma de los grados de los factores.

BIBLIOGRAFÍA

[1] ALBIS, V. *Temas de aritmética y álgebra*. Bogotá, Universidad Nacional de Colombia. 1984.

[2] BEREZIN, F. *Introduction to Superanalysis*. MPAM 9, Reidel. 1987.

[3] CASTRO, I. *Temas de teoría de cuerpos, teoría de anillos y números algebraicos.* Tomo I. Bogotá, Universidad Nacional de Colombia. 1987.

[4] DUBREIL, P.; DUBREIL – JACOTIN, M. *Lecciones de álgebra moderna*. Barcelona, Reverté. 1965.

[5] FRALEIGH, J. *A first course in abstract algebra*. *Sixth edition.* New York, Addison – Wesley. 1999.

[6] HERSTEIN, I. *Álgebra moderna*. México, F. Trillas. 1970.

[7] HILBERT, D. *Fundamentos de la Geometría*. Madrid, Publicaciones del Instituto Jorge Juan de Matemáticas. 1953.

[8] ILSE, D; LEHMANN, I.; SCHULZ, W. *Gruppoide und funktionalgleichungen.* Berlin, VEB Deutscher Verlag der Wissenschaften. 1984.

[9] LENTIN, A.; RIVAUD, J. *Álgebra moderna*. Madrid, Aguilar. 1971.

[10] LUQUE, C. *El cálculo: una versión sin el concepto de límite.* Bogotá, Universidad Pedagógica Nacional. 1993.

[11] LUQUE, C.; DUQUE, O. "Introducción a las álgebras de Grassmann", en: *Memorias del VII Encuentro de Geometría y sus aplicaciones*. Bogotá, Universidad Pedagógica Nacional. pp. 227 – 252. 1996.

[12] PÉREZ, E. *Estructuras algebraicas*. Notas de Clase. Bogotá, Universidad Pedagógica Nacional. 2003.

[13] YAGLOM, I. *A simple non euclidean geometry and its physical basis.* New York, Springer – Verlag. 1979.

Sitios Consultados en Internet

http://mathworld.wolfram.com/